

Guía Portátil Cisco

CCNA Discovery

Diseño y soporte de redes de computadoras

Versión 4.0

ciscopress.com

Cisco | Networking Academy
Mind Wide Open

Guía Portátil Cisco CCNA Discovery **Diseño y soporte de redes de computadoras** Versión 4.0

Traducción autorizada de la obra en inglés titulada COURSE BOOKLET FOR CCNA DISCOVERY DESIGNING AND SUPPORTING COMPUTER NETWORKS, VERSION 4.01.

Authorized translation from the English language edition, entitled COURSE BOOKLET FOR CCNA DISCOVERY DESIGNING AND SUPPORTING COMPUTER NETWORKS, VERSION 4.01, 1st Edition by CISCO NETWORKING ACADEMY, published by Pearson Education, Inc, publishing as Cisco Press, Copyright © 2010 Cisco Systems, Inc.
ISBN-13: 978-1-58713-257-5
ISBN-10: 1-58713-257-5

Atlacomulco 500, 5º piso
Col. Industrial Atoto
C.P. 53519, Naucalpan de Juárez, Edo. de México
Cámara Nacional de la Industria Editorial Mexicana Reg. Núm. 1031

ISBN: 978-607-32-0426-2

Advertencia y exención de responsabilidad

Este libro proporciona información sobre el diseño y soporte de redes de computadoras. Hemos hecho nuestro mejor esfuerzo para que este libro sea lo más completo posible, pero esto no implica una garantía ni precisión al respecto.

La información se proporciona "como está". Los autores, Cisco Press y Cisco Systems, Inc, no tendrán ningún tipo de responsabilidad con ninguna persona o entidad, con respecto a cualquier pérdida o daño producido por la información contenida en este libro, o por el uso de los discos o programas que lo acompañen.

Las opiniones expresadas en este libro pertenecen a los autores y no necesariamente reflejan las de Cisco Systems, Inc.

Editor
Paul Boger

Editor asociado
Dave Dusthimer

Representante de Cisco
Erik Ullanderson

Director del programa Cisco Press
Anand Sundaram

Editor ejecutivo
Mary Beth Ray

Jefe de redacción
Patrick Kanouse

Editor del proyecto
Bethany Wall

Asistente editorial
Vanessa Evans

Diseño de portada
Louisa Adair

Formación
Mark Shirar

Reconocimiento de marcas registradas

Todos los términos que se mencionan en este libro y que sean marcas registradas o marcas de servicio reconocidas están escritas en mayúsculas, según sea apropiado. Ni Cisco Press ni Cisco Systems, Inc. pueden avalar la precisión de esta información. La forma en que se usó un término en este libro no debe afectar la validez de cualquier marca registrada o marca de servicio.

Retroalimentación de información

En Cisco Press, nuestro objetivo es crear libros técnicos de la más alta calidad y valor. Cada libro es diseñado con gran cuidado y precisión, bajo una rigurosa supervisión en la que interviene la experiencia única de los miembros de la comunidad técnica profesional.

Los comentarios de nuestros lectores son una continuación natural de este proceso. Si tiene algún comentario sobre cómo podríamos mejorar la calidad de este libro, o hacer alguna modificación para que se adapte mejor a sus necesidades, contáctenos por correo electrónico en feedback@ciscopress.com. Por favor, asegúrese de incluir el título del libro y el ISBN en su mensaje.

Apreciaremos mucho sus comentarios.

Resumen de contenido

Contenido

Convención de la sintaxis de los comandos utilizados en este libro

La convención utilizada para presentar la sintaxis de los comandos en este libro es la misma que se emplea en el IOS Command Reference, el cual la describe de la siguiente manera:

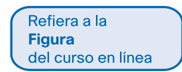
- **Negrita** indica comandos y palabras clave que se escribieron literalmente tal como se presentan. En la salida y los ejemplos de configuración reales (no la sintaxis de comandos generales), el texto en negritas indica comandos que son introducidos manualmente por el usuario (como el comando **mostrar**).
- *Itálica* indica argumentos para los cuales usted debe proporcionar valores reales.
- Barras verticales (|) separan elementos alternativos mutuamente exclusivos.
- Corchetes ([ ]) indican un elemento opcional.
- Llaves ({ }) indican que se requiere una opción.
- Llaves dentro de corchetes ([{ }]) indican que se requiere una opción dentro de un elemento opcional.

Acerca de este libro

Su *Guía Portátil Cisco* de Cisco Networking Academy es una forma de leer el texto del curso sin estar conectado a Internet.

Gracias a su diseño como recurso de estudio, puede leer, resaltar y repasar con facilidad mientras se desplaza de un lado a otro, en donde no haya una conexión disponible a Internet o no sea práctico:

- El texto se extrae de manera directa, palabra por palabra, del curso en línea, para que usted pueda resaltar los puntos importantes.
- Los encabezados con su correlación exacta de página ofrecen una rápida referencia al curso en línea para su análisis en el salón de clases y al prepararse para los exámenes.
- Un sistema de iconos lo lleva al plan de estudios en línea, para que aproveche al máximo las imágenes, laboratorios, actividades de Packet Tracer y las actividades dinámicas basadas en Flash que están incrustadas dentro de la interfaz del curso en línea de la Cisco Networking Academy.



Refiera a la **actividad de laboratorio** del curso en línea

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Refiera al **Gráfico Interactivo** del curso en línea

Vaya al curso en línea y complete la prueba

La *Guía Portátil Cisco* es un recurso rápido, con un enfoque en el ahorro de papel, que lo ayudará a alcanzar el éxito en el curso en línea de Cisco Networking Academy.

Introducción al curso

Bienvenido

Bienvenidos al curso CCNA Discovery, Diseño y soporte de redes de computadoras. El objetivo de este curso es ayudarlo a desarrollar las aptitudes necesarias para diseñar redes LAN y WAN para empresas pequeñas. El curso proporciona una introducción a la recopilación de requisitos del cliente, la traducción de esos requisitos en necesidades de equipos y protocolos, y la creación de una topología de red dirigida a las necesidades del cliente. También los familiarizará con la manera de crear e implementar una propuesta de diseño para un cliente. Este curso le brinda las habilidades necesarias para las tareas de soporte de venta previa de nivel inicial y diseño de redes de nivel inicial.

Más que sólo información

Este ambiente de aprendizaje asistido por PC es una parte importante de la experiencia total del curso para estudiantes e instructores de Networking Academy. Este material en línea del curso está diseñado para utilizarse junto con muchas otras herramientas y actividades instructivas. Por ejemplo:

- Presentaciones en clase, debates y prácticas con su profesor.
- Prácticas de laboratorio que usan equipos de redes dentro del aula de Networking Academy.
- Evaluaciones en línea y un libro de calificaciones.
- La herramienta de simulación Packet Tracer 4.1.
- Software adicional para actividades en clase.

Una comunidad global

Cuando participa en Networking Academy, se suma a una comunidad global conectada por tecnologías y objetivos en común. Participan del programa escuelas en más de 160 países. Para ver un mapa de red interactivo de la comunidad mundial de Networking Academy, visite http://www.academynetspace.com.

El material de este curso versa sobre una gama de tecnologías que facilitan el modo en que las personas trabajan, viven, juegan y aprenden comunicándose con voz, video y otros datos. Hemos trabajado con instructores de todo el mundo para crear este material. Es importante que trabaje con su instructor y sus compañeros para adaptar el material de este curso a su situación local.

Mantenga la comunicación

El material de instrucción en línea y el resto de las herramientas del curso son parte de algo más grande: la Networking Academy de Cisco. El portal del programa se encuentra en http://www.cisco.com/web/learning/netacad/index.html. Mediante este portal usted accede a herramientas, actualizaciones de información y otros enlaces importantes, entre ellos el servidor de evaluación y el libro de calificaciones del estudiante.

Mind Wide Open™

Un objetivo importante en la educación es enriquecer al estudiante (a usted), ampliando lo que sabe y puede hacer. Sin embargo, es importante comprender que el material de instrucción y el instructor sólo pueden facilitarle el cambio. Usted debe comprometerse a aprender nuevas aptitudes. A continuación encontrará algunas sugerencias que facilitarán su aprendizaje:

1. **Tome notas**. Los profesionales del campo de red generalmente tienen diarios de ingeniería en donde anotan lo que observan y aprenden. La toma de notas es una forma importante de lograr que su conocimiento mejore con el tiempo.
2. **Piense en lo que observa y aprende**. El curso le brinda información para cambiar lo que sabe y lo que puede hacer. A medida que el curso avanza, pregúntese qué tiene sentido y qué no. Deténgase y haga preguntas cuando esté confundido. Intente averiguar más sobre los temas que le interesan. Si no está seguro por qué se enseña algo, pregúntele a su instructor o a un amigo. Piense cómo se complementan las distintas partes del curso.
3. **Practique**. Aprender nuevas aptitudes requiere de práctica. Creemos que practicar es tan importante para el e-learning que le dimos un nombre especial. Lo llamamos e-Doing. Es muy importante que realice las actividades del material de instrucción en línea y que realice las actividades del Packet Tracer® y las prácticas de laboratorio.
4. **Practique de nuevo**. ¿Alguna vez pensó que sabía cómo hacer algo y luego, cuando llegó el momento de demostrarlo en una prueba o en el trabajo, descubrió que en realidad no había aprendido bien cómo hacerlo? Como cuando se aprende cualquier nueva habilidad, como un deporte, un juego o un idioma, aprender una aptitud profesional requiere paciencia y mucha práctica antes de que pueda decir que realmente la ha aprendido. El material de instrucción en línea de este curso le brinda oportunidades para practicar mucho distintas aptitudes. Aprovéchelas al máximo. Trabaje con su instructor para crear oportunidades de práctica adicionales con el Packet Tracer y otras herramientas.
5. **Enseñe**. Generalmente, enseñarle a un amigo o colega es una buena forma de mejorar su propio aprendizaje. Para enseñar bien, debe completar los detalles que puede haber pasado por alto en la primera lectura. Las conversaciones sobre el material del curso con compañeros, colegas y el instructor pueden ayudarlo a fijar los conocimientos de los conceptos de red.
6. **Realice cambios a medida que avanza**. El curso está diseñado para proporcionar comentarios mediante actividades y cuestionarios interactivos, el sistema de evaluación en línea y a través de interacciones con su instructor. Puede utilizar estos comentarios para entender mejor cuáles son sus fortalezas y debilidades. Si existe un área en la que tiene problemas, concéntrese en estudiar o practicar más esa área. Solicite comentarios a su instructor y a otros estudiantes.

Explore el mundo de networking

Esta versión del curso incluye una herramienta de aprendizaje especial llamada Packet Tracer 4.1®. El Packet Tracer admite una amplia gama de simulacros físicos y lógicos, además de brindar herramientas de visualización para ayudarlo a entender los trabajos internos de una red.

Las actividades del Packet Tracer que vienen con este curso consisten en simulacros de red, juegos, actividades y desafíos que proporcionan una amplia variedad de experiencias de aprendizaje.

Cree sus propios mundos

También puede usar el Packet Tracer para crear sus propios experimentos y situaciones de red. Esperamos que, con el tiempo, considere utilizar el Packet Tracer no sólo para experimentar las actividades provistas, sino también para convertirse en autor, explorador y experimentador.

Las actividades incluidas del Packet Tracer se inician en computadoras con sistema operativo Windows®, si el Packet Tracer está instalado. Esta integración también puede funcionar en otros sistemas operativos que usan la emulación de Windows.

Cada vez es más frecuente la interacción e intercambio de ideas mediante una red basada en servicio IP. Detrás de escena, los diseñadores de redes son los arquitectos de este cambio drástico en la manera de comunicarnos.

Necesitamos redes convergentes que puedan crecer y adecuarse a las crecientes demandas de nuevos servicios. Esperamos que las aplicaciones y los servicios de red que usamos estén disponibles y sean seguros. Además, a medida que las redes subyacentes se vuelven más complejas, el soporte y la administración de estas redes se convierten en una prioridad absoluta. Confiamos en los diseñadores de red para que nuestras redes puedan alcanzar nuestras expectativas.

Una red bien diseñada protege nuestra inversión en tecnología de red y brinda ventaja competitiva a nuestras organizaciones. Las oportunidades laborales en el diseño de redes crecen rápidamente a medida que las grandes y pequeñas organizaciones comprenden la importancia de crear redes sobre la base sólida de un buen diseño.

Al completar exitosamente este curso, usted aprenderá:

- La finalidad de un buen diseño de red.
- A utilizar el método Life Cycle Services de Cisco en un proyecto de diseño de red.
- Técnicas para describir una red existente para prepararla para una actualización.
- El impacto de las distintas aplicaciones y los distintos servicios en el diseño de red.
- Los requisitos de diseño de las capas núcleo, de distribución y de acceso del campus, incluidos el acceso inalámbrico y la seguridad.
- Los requisitos de diseño de la conectividad WAN de Enterprise Edge y el soporte VPN para trabajadores remotos.
- El proceso para probar y validar la red del campus y el diseño de la WAN.
- La preparación y presentación de una propuesta de actualización de red.

CAPÍTULO 1

Introducción de conceptos de diseño de red

Introducción

Refiera a la **Figura** del curso en línea

1.1 Descubrimiento de principios básicos de diseño de red

1.1.1 Descripción general del diseño de red

Refiera a la **Figura** del curso en línea

Las computadoras y las redes de información son esenciales para lograr el éxito en empresas grandes o pequeñas. Éstas conectan a las personas, admiten aplicaciones y servicios, y proporcionan acceso a los recursos que mantienen el funcionamiento de las empresas. Para cumplir con los requisitos diarios de las empresas, las redes se están volviendo bastante complejas.

Requisitos de la red

En la actualidad, la economía basada en Internet a menudo demanda un servicio al cliente las 24 horas. Esto significa que las redes comerciales deben estar disponibles casi el 100% del tiempo. Deben ser lo suficientemente inteligentes como para protegerse automáticamente de los incidentes de seguridad imprevistos. Estas redes comerciales también deben poder adaptarse a las cargas de tráfico cambiantes para mantener tiempos de respuesta constantes en las aplicaciones. Ya no se considera práctico crear redes mediante la conexión de varios componentes independientes sin contar con un diseño y una planificación detallada.

Creación de una red eficiente

Las redes eficientes no existen por casualidad. Son el resultado del arduo trabajo de técnicos y diseñadores de red, quienes identifican los requisitos de la red y seleccionan las mejores soluciones para satisfacer las necesidades de una empresa.

Refiera a la **Figura** del curso en línea

En general, los usuarios de la red no piensan en términos de complejidad de la red subyacente. Consideran la red como una forma de acceder a las aplicaciones que necesitan, cuando lo necesitan.

Requisitos de la red

En la actualidad, la mayoría de las empresas sólo incluye algunos requisitos para su red:

- La red debe estar activa a toda hora, incluso en caso de falla en los enlaces, en el equipo y en condiciones de sobrecarga.
- También debe entregar aplicaciones de manera confiable y proporcionar tiempos de respuesta razonables de host a host.
- Debe ser segura. Debe proteger los datos que se transmiten a través de la misma, al igual que los datos almacenados en los dispositivos que se conectan a ella.
- La red debe ser fácil de modificar para adaptarse al crecimiento de la red y a los cambios generales de la empresa.

- La resolución de problemas debe ser sencilla, ya que las fallas ocurren con frecuencia. La detección y resolución de un problema no debe llevar demasiado tiempo.

Objetivos fundamentales del diseño

Al analizarlos detenidamente, estos requisitos se resumen en cuatro objetivos fundamentales del diseño de red:

- Escalabilidad
- Disponibilidad
- Seguridad
- Facilidad de administración

1.1.2 Beneficios de un diseño jerárquico de red

Refiera a la **Figura** del curso en línea

Para cumplir con los cuatro objetivos fundamentales del diseño, la red se debe fundamentar sobre una arquitectura que permita la flexibilidad y el crecimiento.

Diseño jerárquico de red

En el sistema de redes se utiliza un diseño jerárquico para agrupar los dispositivos en varias redes. Las redes se organizan mediante un enfoque de capas. El modelo de diseño jerárquico tiene tres capas básicas:

- ***Capa núcleo:*** conecta los dispositivos de la capa de distribución
- ***Capa de distribución:*** interconecta las redes locales más pequeñas
- ***Capa de acceso:*** proporciona conectividad para los hosts de la red y los dispositivos finales

Ventajas sobre las redes planas

Las redes jerárquicas poseen ventajas sobre los diseños de red plana. El beneficio de dividir una red plana en bloques más pequeños y fáciles de administrar es que el tráfico local sigue siendo local. Sólo el tráfico destinado a otras redes se traslada a una capa superior.

Los dispositivos de Capa 2 en una red plana brindan pocas oportunidades de controlar broadcasts o filtrar tráfico no deseado. A medida que se agregan más dispositivos y aplicaciones a una red plana, los tiempos de respuesta se degradan hasta que la red queda inutilizable.

Refiera a la **Figura** del curso en línea

Las ***Arquitecturas empresariales de Cisco*** pueden utilizarse para dividir aún más el diseño jerárquico de tres capas en áreas modulares. Los módulos representan áreas que tienen una conectividad física o lógica diferente. Se encargan de designar dónde se llevan a cabo las diferentes funciones en la red. Esta modularidad permite la flexibilidad en el diseño de la red. Facilita la implementación y la resolución de problemas. Las tres áreas de enfoque en el diseño modular de red son:

- ***Campus empresarial:*** esta área contiene los elementos de red que se requieren para una operación independiente dentro de un solo campus o sucursal.
- ***Granja de servidores:*** es un componente del campus empresarial; la granja de servidores del centro de datos protege los recursos del servidor y proporciona una conectividad de alta velocidad redundante y confiable.
- ***Margen empresarial:*** a medida que el tráfico ingresa a la red del campus, esta área filtra el tráfico de los recursos externos y los enruta hacia la red empresarial. Contiene todos los

elementos requeridos para lograr una comunicación eficiente y segura entre el campus empresarial y las ubicaciones remotas, los usuarios remotos e Internet.

Refiera a la **Figura** del curso en línea

El marco de trabajo modular de las arquitecturas empresariales de Cisco incluye las siguientes ventajas de diseño:

- Crea una ***red determinista*** con límites claramente definidos entre los módulos. Esto provee puntos claros de demarcación para que el diseñador de la red sepa exactamente en dónde se origina el tráfico y dónde fluye.
- Facilita la tarea de diseño al lograr que cada módulo sea independiente. El diseñador puede enfocarse en las necesidades de cada área por separado.
- Proporciona escalabilidad al permitir a las empresas agregar módulos fácilmente. A medida que aumenta la complejidad de la red, el diseñador puede agregar nuevos módulos funcionales.
- Permite al diseñador agregar servicios y soluciones sin cambiar el diseño de la red subyacente.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastre las características del modelo jerárquico y las arquitecturas empresariales de Cisco hacia las ubicaciones correctas y luego haga clic en Verificar.

1.1.3 Metodologías del diseño de red

Refiera a la **Figura** del curso en línea

Los grandes proyectos de diseño de red generalmente se dividen en tres pasos distintos:

Paso 1: Identifique los requisitos de la red.

Paso 2: Caracterice la red existente.

Paso 3: Diseñe la topología de red y las soluciones.

Identificación de requisitos de la red

El diseñador de la red trabaja junto con el cliente para documentar los objetivos del proyecto. Los objetivos generalmente se dividen en dos categorías:

- Objetivos comerciales: se enfocan en cómo la red puede lograr un mayor éxito comercial.
- Requisitos técnicos: se enfocan en cómo se implementa la tecnología dentro de la red.

Caracterización de la red existente

Se reúne y se analiza información sobre los servicios y redes actuales. Es necesario comparar la funcionalidad de la red existente con los objetivos del nuevo proyecto definidos. El diseñador determina si el equipo existente, la infraestructura y los protocolos pueden volver a utilizarse, y qué equipo y protocolos nuevos se necesitan para completar el diseño.

Diseño de la topología de la red

Una estrategia común para el diseño de la red es aplicar un ***enfoque descendente***. En este enfoque, se identifican las aplicaciones de la red y los requisitos del servicio. Después, se diseña la red para apoyar dichas aplicaciones y requisitos.

Se realiza un prototipo o prueba de concepto al completar el diseño. Este enfoque asegura que el nuevo diseño funcione según lo previsto antes de su implementación.

Refiera a la **Figura** del curso en línea

Un error común que cometen los diseñadores de la red es no determinar de manera correcta el alcance del proyecto de diseño de la red.

Determinación del alcance del proyecto

Al reunir los requisitos, el diseñador identifica los problemas que afectan a toda la red y aquellos que afectan sólo a partes específicas. A menudo, el alcance del proyecto se expande más allá del cálculo original al no comprender el impacto de un requisito particular. Esta equivocación puede aumentar en gran medida el costo y tiempo requeridos para implementar el nuevo diseño.

Impacto en toda la red

Los requisitos que afectan a toda la red incluyen:

- Agregar nuevas aplicaciones de red y realizar cambios importantes en las aplicaciones existentes, como cambios en la base de datos o en la estructura DNS
- Mejorar la eficiencia de los cambios en el protocolo de direccionamiento y enrutamiento de la red
- Integrar nuevas medidas de seguridad
- Agregar nuevos servicios de red, como por ejemplo el tráfico de voz, ***networking de contenidos*** y ***networking de almacenamiento***
- Reubicar servidores en una granja de servidores del centro de datos

Refiera a la **Figura** del curso en línea

Impacto en la porción de la red

Entre los requisitos que sólo pueden afectar una porción de la red se incluyen:

- Mejorar la conectividad de Internet y agregar ancho de banda
- Actualizar el cableado LAN de la capa de acceso
- Proporcionar redundancia para los servicios clave
- Dar apoyo al acceso inalámbrico en áreas definidas
- Actualizar el ancho de banda de la WAN

Probablemente estos requisitos no afecten a muchos usuarios ni requieran de varios cambios en el equipo instalado. A veces es posible integrar los cambios de diseño en la red existente sin interrumpir las operaciones normales de la red para la mayoría de sus usuarios. Este método reduce los costos asociados con el tiempo de inactividad y acelera la implementación de la actualización de la red.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad

Determine si el requisito afecta toda la red o sólo una porción de la misma marcando la columna adecuada. Después haga clic en Verificar.

1.2 Investigación de las consideraciones del diseño de la capa núcleo

1.2.1 ¿Qué sucede en la capa núcleo?

Refiera a la **Figura** del curso en línea

La capa núcleo a menudo se denomina ***backbone de la red***. Los routers y los switches en la capa núcleo proporcionan conectividad de alta velocidad. En una LAN empresarial, la capa núcleo puede conectar múltiples edificios o sitios, además de proporcionar conectividad a la granja de servidores. La capa núcleo incluye uno o más enlaces a los dispositivos en el margen empresarial a fin de admitir Internet, ***redes privadas virtuales (VPN)***, ***extranet*** y acceso a la WAN.

La implementación de una capa núcleo reduce la complejidad de la red, lo cual facilita la administración y la resolución de problemas.

Objetivos de la capa núcleo

El diseño de la capa núcleo permite la transferencia de datos eficiente y de alta velocidad entre una y otra sección de la red. Los objetivos principales del diseño en la capa núcleo son:

- Proporcionar un 100% de tiempo de actividad
- Maximizar el rendimiento
- Facilitar el crecimiento de la red

Tecnologías de capa núcleo

Entre las tecnologías que se utilizan en la capa núcleo se incluyen:

- Routers o ***switches multicapa*** que combinan el enrutamiento y la conmutación en el mismo dispositivo
- Redundancia y ***balanceo de carga***
- Enlaces de alta velocidad y agregados
- Protocolos de enrutamiento escalables y de rápida convergencia, como el Protocolo de enrutamiento de gateway interior mejorado (***EIGRP***) y el protocolo Abrir primero el camino más corto (***OSPF***)

Enlaces redundantes

Refiera a la **Figura** del curso en línea

La implementación de enlaces redundantes en la capa núcleo garantiza que los dispositivos de red puedan encontrar caminos alternativos para enviar datos en caso de falla. Cuando los dispositivos de la Capa 3 se colocan en la capa núcleo, estos enlaces redundantes pueden utilizarse para realizar el balanceo de carga, además de proporcionar respaldo. En un diseño de red plana de Capa 2, el ***Protocolo Spanning Tree (STP)*** deshabilita los enlaces redundantes, a menos que falle un enlace principal. Este comportamiento del STP previene el balanceo de carga sobre los enlaces redundantes.

Topología de malla

La mayoría de las capas núcleo de una red se conectan en una topología de ***malla completa*** o ***malla parcial***. Una topología de malla completa es donde cada dispositivo posee una conexión con los demás dispositivos. Si bien las topologías de malla completa proporcionan la ventaja de una red completamente redundante, éstas pueden ser difíciles de conectar y administrar y son más costosas. Para las instalaciones más grandes, se utiliza una topología de malla parcial modificada. En una topología de malla parcial, cada dispositivo se conecta al menos a otros dos dispositivos, lo cual crea una redundancia suficiente sin la complejidad de una malla completa.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Crear y comparar topologías de malla parcial y completa entre los routers.

1.2.2 Prioridad del tráfico de la red

Refiera a la **Figura** del curso en línea

Prevención de fallas

El diseñador de la red debe esforzarse por proporcionar una red que sea resistente a las fallas y que pueda recuperarse rápidamente en caso de falla. Los switches y routers centrales pueden contener:

- Ventiladores y fuentes de energía dobles
- Un diseño modular con base en chasis
- Módulos de administración adicionales

Los componentes redundantes aumentan el costo, pero generalmente vale la pena invertir en ellos. Los dispositivos de la capa núcleo deben poseer componentes ***intercambiables en caliente*** cuando sea posible. Los componentes intercambiables en caliente pueden instalarse o retirarse sin tener que interrumpir primero la potencia del dispositivo. El uso de estos componentes reduce el tiempo de reparación y la interrupción de los servicios de red.

Las empresas más grandes a menudo instalan generadores y dispositivos ***UPS*** grandes. Estos dispositivos evitan que los cortes leves de energía eléctrica causen fallas en redes a gran escala.

Reducción del error humano

Los errores humanos contribuyen a las fallas en la red. Lamentablemente, estos factores no pueden eliminarse al agregar equipo y enlaces redundantes. Muchas fallas de la red son el resultado de actualizaciones o adiciones mal planificadas y sin probar al nuevo equipo. ¡Nunca realice un cambio de configuración en una red de producción sin probarlo primero en un entorno de laboratorio!

Las fallas en la capa núcleo provocan interrupciones generalizadas. Es esencial contar con procedimientos y políticas adecuadas por escrito para determinar de qué manera se deben autorizar, probar, aplicar y documentar los cambios. Planifique una estrategia de retirada para regresar la red a su estado anterior si los cambios no producen el resultado esperado.

1.2.3 Convergencia de red

Refiera a la **Figura** del curso en línea

La elección de un protocolo de enrutamiento para la capa núcleo se determina mediante el tamaño de la red y la cantidad de enlaces redundantes o rutas disponibles. Un factor principal al elegir un protocolo es la rapidez con la que se recupera de una falla en el dispositivo o enlace.

Convergencia

La convergencia de red se produce cuando todos los routers tienen información completa y precisa sobre la red. Mientras más breve sea el ***tiempo de convergencia***, más rápido podrá reaccionar una red ante un cambio en la topología. Entre los factores que afectan el tiempo de convergencia se incluyen:

- La velocidad con la cual las actualizaciones de enrutamiento alcanzan a todos los routers de la red
- El tiempo que se demora cada router en realizar el cálculo a fin de determinar las mejores rutas

Selección de un protocolo de enrutamiento

La mayoría de los protocolos de enrutamiento dinámico ofrecen tiempos de convergencia aceptables en las redes pequeñas. En redes más grandes, los protocolos como RIPv2 pueden converger muy lentamente para evitar una interrupción en los servicios de la red cuanto un enlace falla. Por lo general, en una red empresarial grande, el EIGRP o el OSPF proporcionan la solución de enrutamiento más estable.

Consideraciones de diseño

La mayoría de las redes contienen una combinación de rutas estáticas y dinámicas. Los diseñadores de red deben considerar la cantidad de rutas necesarias para asegurarse de que puedan alcanzarse todos los destinos en la red. La convergencia de las tablas de enrutamiento grandes puede demorar un tiempo considerable. El diseño de direccionamiento de red y estrategias de sumarización en todas las capas afecta la eficiencia con la que el protocolo de enrutamiento puede reaccionar ante una falla.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Utilizando la topología existente, agregar un nuevo segmento LAN para observar la convergencia de la red.

1.3 Investigación de las consideraciones de la capa de distribución

1.3.1 ¿Qué sucede en la capa de distribución?

Refiera a la **Figura** del curso en línea

La capa de distribución representa un límite de enrutamiento entre la capa de acceso y la capa núcleo. También sirve como punto de conexión entre los sitios remotos y la capa núcleo.

Enrutamiento de la capa de distribución

La capa de acceso comúnmente se crea utilizando una tecnología de conmutación de Capa 2. La capa de distribución se crea utilizando dispositivos de Capa 3. Los routers o switches multicapa, ubicados en la capa de distribución, proporcionan muchas funciones que son esenciales para cumplir con los objetivos del diseño de red. Estos objetivos incluyen:

- Filtrar y administrar los flujos del tráfico
- Exigir el cumplimiento de las políticas de control de acceso
- Resumir rutas antes de publicarlas en el núcleo
- Aislar el núcleo de las interrupciones o fallas de la capa de acceso
- Enrutar entre las VLAN de la capa de acceso

Los dispositivos de la capa de distribución también se utilizan para administrar colas y priorizar el tráfico antes de realizar la transmisión a través del núcleo del campus.

Refiera a la **Figura** del curso en línea

Enlaces troncales

Los enlaces troncales a menudo se configuran entre los dispositivos de red de la capa de distribución y de acceso. También se utilizan para transportar tráfico que pertenece a múltiples VLAN entre dispositivos a través del mismo enlace. Al diseñar los enlaces troncales, el diseñador de red considera los patrones de tráfico de la red y la estrategia VLAN generales.

Enlaces redundantes

Cuando existen enlaces redundantes entre los dispositivos de la capa de distribución, estos dispositivos pueden configurarse para balancear la carga del tráfico a través de los enlaces. El balanceo de carga aumenta el ancho de banda disponible para las aplicaciones.

Topología de la capa de distribución

Las redes de la capa de distribución generalmente se conectan en una topología de malla parcial. Esta topología proporciona suficientes rutas redundantes como para asegurar que la red pueda sobrevivir a una falla en el dispositivo o enlace. Cuando los dispositivos de la capa de distribución se ubican en el mismo armario de cableado o centro de datos, éstos se interconectan utilizando enlaces Gigabit. Cuando los dispositivos están separados por distancias más grandes, se utiliza cable de fibra. Los switches que admiten múltiples conexiones de fibra de alta velocidad pueden ser costosos. Por lo tanto, es necesaria una planificación detallada para garantizar que existan suficientes puertos de fibra disponibles a fin de proporcionar la redundancia y el ancho de banda deseados.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Demostrar las funciones realizadas por los dispositivos de la capa de distribución.

1.3.2 Limitación del alcance de fallas en la red

Refiera a la **Figura** del curso en línea

Un dominio de fallas define la porción de la red que se ve afectada cuando falla una aplicación de red o dispositivo.

Limitación del tamaño de los dominios de fallas

El diseñador de red a menudo se centra en tratar de evitar fallas, ya que éstas afectan de manera considerable la capa núcleo de una red. Estos esfuerzos pueden aumentar en gran medida el costo para implementar la red. En el modelo de diseño jerárquico, es más fácil y generalmente menos costoso controlar el tamaño de un dominio de fallas en la capa de distribución. En la capa de distribución, los errores de la red pueden contenerse en un área más pequeña y así afectar a la menor cantidad de usuarios. Al utilizar los dispositivos de Capa 3 en la capa de distribución, cada router funciona como gateway para una cantidad limitada de usuarios de la capa de acceso.

Implementación de bloques de switches

Los routers o switches multicapa generalmente se implementan en pares, con switches de capa de acceso divididos en forma equitativa entre los mismos. Esta configuración se denomina ***bloque de switch*** de departamento o construcción. Cada bloque de switches funciona de manera independiente. Como resultado, la falla de un único dispositivo no desactiva la red. Incluso la falla de todo un bloque de switches no afecta a un número considerable de usuarios finales.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Apagar los dispositivos y desactivar las interfaces para ver las fallas resultantes de la red.

1.3.3 Creación de una red redundante

Refiera a la **Figura** del curso en línea

Para reducir el tiempo de inactividad, el diseñador de red implementa redundancia en la red.

Redundancia en la capa de distribución

Los dispositivos en la capa de distribución tienen conexiones redundantes con los switches en la capa de acceso y con los dispositivos en la capa núcleo. Si falla un dispositivo o un enlace, estas conexiones proporcionan rutas alternativas. Al utilizar un protocolo de enrutamiento adecuado en la capa de distribución, los dispositivos de Capa 3 reaccionan rápidamente ante las fallas en los enlaces; por lo tanto, no afectan el funcionamiento de la red.

La utilización de varias conexiones con los switches de Capa 2 puede provocar un comportamiento inestable en una red a menos que se active el STP. Sin el STP, los enlaces redundantes en una red de Capa 2 pueden causar tormentas de broadcast. Los switches no son capaces de aprender de forma correcta los puertos; por lo tanto, el tráfico termina acumulándose en todo el switch. Al deshabilitar uno de los enlaces, el STP garantiza que sólo esté activa una ruta entre dos dispositivos. Si falla uno de los enlaces, el switch vuelve a calcular la topología de árbol de expansión y comienza a utilizar automáticamente el enlace alternativo.

El Protocolo rápido de árbol de expansión (RSTP, Rapid Spanning Tree Protocol), según se define en IEEE 802.1w, se basa en la tecnología IEEE 802.1d y proporciona una rápida convergencia del árbol de expansión.

Refiera a la **Figura** del curso en línea

Un servidor empresarial de gran volumen se conecta a un puerto del switch. Si dicho puerto realiza un nuevo cálculo debido al STP, el servidor se desconecta durante 50 segundos. Sería difícil imaginar la cantidad de transacciones perdidas durante dicho plazo.

En una red estable, son poco frecuentes los nuevos cálculos del STP. En una red inestable, es importante verificar los switches para detectar cambios en la configuración y la estabilidad. Una de las causas más comunes de los nuevos cálculos del STP en forma frecuente es la falla en una fuente de energía o suministro eléctrico del switch. Una fuente de energía defectuosa provoca el reinicio del dispositivo de manera imprevista.

1.3.4 Filtrado del tráfico en la capa de distribución

Las ***listas de control de acceso (ACL, Access control lists)*** representan una herramienta que puede utilizarse en la capa de distribución para limitar el acceso y evitar que el tráfico no deseado ingrese a la red de núcleo. Una ACL es una lista de condiciones que se utilizan para probar el tráfico de la red que intenta viajar a través de la interfaz del router. Las declaraciones de la ACL identifican qué paquetes aceptar o denegar.

Filtrado del tráfico de la red

Para filtrar el tráfico de la red, el router examina cada paquete y luego lo envía o lo descarta, según las condiciones especificadas en la ACL. Existen diferentes tipos de ACL para distintos propósitos. Las ACL estándar filtran el tráfico según la dirección de origen. Las ACL extendidas pueden filtrar según varios criterios, entre ellos:

- Dirección de origen
- Dirección de destino
- Protocolos
- Números de puerto o aplicaciones
- Si el paquete es parte de un flujo TCP establecido

Tanto las ACL estándar como las extendidas pueden configurarse como listas de acceso por nombre o por número.

ACL complejas

Las ACL extendidas y estándar sirven de base para otras clases de ACL más complejas. Con el software IOS de Cisco, se pueden configurar tres funciones de ACL compleja: dinámica, reflexiva y basada en tiempo.

ACL dinámica: requiere que un usuario utilice Telnet para conectarse al router y realizar la autenticación. Una vez autenticada, se permite el tráfico proveniente del usuario. A menudo, las ACL dinámicas se denominan “lock and key” (bajo llave) porque el usuario debe iniciar sesión para poder obtener acceso.

ACL reflexiva: permite el tráfico saliente y luego limita el tráfico entrante de manera que se admitan sólo las respuestas a solicitudes autorizadas. Es similar a la palabra clave `established` que se utiliza en las declaraciones ACL extendidas, excepto que estas ACL también pueden inspeccionar el tráfico ICMP y UDP, además de TCP.

ACL basada en tiempo: permite y deniega determinado tráfico según la hora del día o el día de la semana.

Ubicación de las ACL

Refiera a la **Figura** del curso en línea

El tráfico que viaja hacia una interfaz se filtra mediante la ACL entrante. El tráfico que sale de una interfaz se filtra mediante la lista de control de acceso saliente. El diseñador de red debe decidir dónde ubicar las ACL dentro de la red para alcanzar los resultados deseados.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastre la ACL correcta hacia la declaración correspondiente y luego haga clic en Verificar.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Ubicar las ACL en la interfaz adecuada dentro de la topología.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear una ACL para cumplir con las condiciones especificadas en la práctica de laboratorio.

1.3.5 Protocolos de enrutamiento en la capa de distribución

Refiera a la **Figura** del curso en línea

Otra función importante que tiene lugar en la capa de distribución es la sumarización de ruta, también denominada agregación de ruta o creación de superredes.

Sumarización de ruta

La sumarización de ruta posee varias ventajas para la red, por ejemplo:

- Una ruta en la tabla de enrutamiento que representa a muchas otras rutas, lo cual crea tablas de enrutamiento más pequeñas
- Menor tráfico de actualización de enrutamiento en la red
- Sobrecarga inferior en el router

La sumarización puede realizarse en forma manual o automática, según el tipo de protocolo de enrutamiento que se utilice en la red.

Los protocolos de enrutamiento sin clase, como el RIPv2, ***EIGRP***, OSPF e ***IS-IS***, admiten la sumarización de ruta según las direcciones de subred en cualquier límite.

Los protocolos de enrutamiento con clase, como el RIPv1, resumen las rutas en forma automática en el límite de red con clase pero no admiten la sumarización en cualquier otro límite.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastrar el resumen de rutas hacia la ubicación adecuada.

1.4 Investigación de las consideraciones del diseño de capa de acceso

1.4.1 ¿Qué sucede en la capa de acceso?

Refiera a la **Figura** del curso en línea

La capa de acceso representa el extremo de la red donde se conectan los dispositivos finales. Los dispositivos y servicios de la capa de acceso residen dentro de cada edificio de un campus, en cada sitio remoto y granja de servidores, y en el margen empresarial.

Consideraciones físicas de la capa de acceso

La capa de acceso de la infraestructura del campus utiliza la tecnología de conmutación de Capa 2 para proporcionar acceso a la red. El acceso puede ser a través de una infraestructura cableada permanente o mediante puntos de acceso inalámbrico. Ethernet con cableado de cobre implica limitaciones con respecto a la distancia. Por lo tanto, uno de los principales enfoques al diseñar la capa de acceso de una infraestructura del campus es la ubicación física del equipo.

Armarios de cableado

Los armarios de cableado pueden ser armarios reales o cuartos de telecomunicaciones pequeños que funcionan como punto de terminación para el cableado de la infraestructura dentro de edificios o de sus pisos. La colocación y el tamaño físico de los armarios de cableado depende del tamaño de la red y de los planes de expansión.

El equipo del armario de cableado suministra potencia a los dispositivos finales como teléfonos IP y puntos de acceso inalámbrico. Muchos switches de la capa de acceso tienen funcionalidad ***Power-over-Ethernet (PoE)***.

A diferencia de un armario de cableado común, dentro de un conjunto de servidores o centro de datos, los dispositivos de la capa de acceso generalmente son switches multicapa redundantes que combinan la funcionalidad del enrutamiento y la conmutación. Los switches multicapa pueden proporcionar funciones de protección contra intrusos y de firewall, al igual que las funciones de Capa 3.

Refiera a la **Figura** del curso en línea

Impacto de las redes convergentes

La red informática moderna implica mucho más que sólo computadoras personales e impresoras conectadas a la capa de acceso. Muchos dispositivos diferentes pueden conectarse a una red IP, entre ellos:

- Teléfonos IP
- Videocámaras
- Sistemas de videoconferencia

Todos estos dispositivos pueden converger en una única infraestructura física de capa de acceso. Sin embargo, el diseño lógico de la red que se necesita para admitirlos se vuelve más complejo debido a ciertas consideraciones, como la QoS, la segregación de tráfico y el filtrado. Estos nuevos tipos de dispositivos finales, junto con las aplicaciones y los servicios relacionados, modifican los requisitos para la escalabilidad, disponibilidad, seguridad y facilidad de administración en la capa de acceso.

Necesidad de disponibilidad

En las redes más antiguas, la disponibilidad alta por lo general estaba presente solamente en el núcleo de la red, en el margen empresarial y en las redes de centro de datos. Gracias a la telefonía IP, en la actualidad se espera que cada teléfono individual esté disponible el 100% del tiempo.

Los componentes redundantes y las estrategias de ***migración en caso de fallos*** pueden implementarse en la capa de acceso para mejorar la confiabilidad y aumentar la disponibilidad para los dispositivos finales.

Administración de la capa de acceso

Refiera a la **Figura** del curso en línea

Las mejoras en la facilidad de administración de la capa de acceso es de gran interés para el diseñador de red. La administración de la capa de acceso es esencial debido a lo siguiente:

- El aumento en la cantidad y en los tipos de dispositivos que se conectan a la capa de acceso
- La introducción de puntos de acceso inalámbrico dentro de la LAN

Diseño para la facilidad de administración

Además de proporcionar conectividad básica en la capa de acceso, el diseñador necesita considerar lo siguiente:

- Denominación de estructuras
- Arquitectura VLAN

- Patrones de tráfico
- Estrategias de prioridad

La configuración y utilización de sistemas de administración de red son fundamentales para una red convergente grande. También es importante estandarizar configuraciones y equipos cuando sea posible.

El cumplimiento de principios de diseño eficientes mejora la facilidad de administración y el respaldo constante de la red al realizar lo siguiente:

- Garantizar que la red no se vuelva demasiado compleja
- Permitir una resolución de problemas sencilla cuando se presenta un problema
- Facilitar la incorporación de nuevas funciones y servicios en el futuro

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Examinar las diferentes funciones de la capa de acceso.

1.4.2 Topologías de red en la capa de acceso

Refiera a la **Figura** del curso en línea

La mayoría de las redes Ethernet recientes utilizan una topología en estrella que a menudo se denomina topología hub and spoke. En una topología en estrella, cada dispositivo final posee una conexión directa a un único dispositivo de red. Este único dispositivo de red generalmente es un switch multicapa o de Capa 2. Una topología en estrella cableada en la capa de acceso por lo general no tiene redundancia desde los dispositivos finales individuales al switch. Para muchas empresas, el costo del cableado adicional para crear redundancia generalmente es demasiado alto.

Entre las ventajas de una topología en estrella se incluyen:

- Instalación fácil
- Configuración mínima

Las desventajas de una topología en estrella son considerables:

- El dispositivo central representa un punto único de falla.
- Las capacidades del dispositivo central pueden limitar el rendimiento general para acceder a la red.
- La topología no se recupera en caso de falla cuando no existen enlaces redundantes.

Las topologías en estrella Ethernet generalmente poseen una combinación del siguiente cableado:

- Cableado de par trenzado para conectarse a los dispositivos finales individuales
- Fibra para interconectar los switches de acceso a los dispositivos de la capa de distribución

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Crear una topología en estrella de la capa de acceso.

1.4.3 Cómo las VLAN segregan y controlan el tráfico de la red

Utilización de las VLAN para segregar el tráfico

Refiera a la **Figura** del curso en línea

La utilización de las VLAN y subredes IP es el método más común para segregar grupos de usuarios y tráfico dentro de la red de la capa de acceso.

Las VLAN en el pasado

Con la introducción de la conmutación de Capa 2, las VLAN se utilizaron para crear redes de grupo de trabajo de extremo a extremo. Las redes se conectaban a través de edificios o incluso a través de toda la infraestructura. Las VLAN de extremo a extremo ya no se utilizan más de esta manera. El aumento en la cantidad de usuarios y el volumen de tráfico de la red que generan estos usuarios es demasiado alto para ser admitido.

Las VLAN en la actualidad

En la actualidad, las VLAN se utilizan para separar y clasificar flujos de tráfico, además de controlar el tráfico de broadcast dentro de un único armario de cableado o edificio. Si bien las VLAN grandes que abarcan redes enteras ya no son recomendables, éstas pueden ser necesarias para admitir aplicaciones especiales, como servicios de roaming y teléfonos IP inalámbricos.

El método recomendado es contener las VLAN dentro de un único armario de cableado. Este método aumenta la cantidad de VLAN en una red, lo cual también incrementa el número de subredes IP individuales. Se recomienda asociar una única subred IP con una única VLAN. El direccionamiento IP en la capa de acceso pasa a ser un aspecto de diseño esencial que afecta la escalabilidad de toda la red.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Monitorear el tráfico que pasa a través de una VLAN.

1.4.4 Servicios en el extremo de la red

Provisión de Calidad de servicio en las aplicaciones de red

Refiera a la **Figura** del curso en línea

Las redes deben prestar servicios seguros, predecibles, medibles y, a veces, garantizados. Las redes también necesitan mecanismos para controlar la congestión cuando aumenta el tráfico. La congestión se produce cuando la demanda de recursos de red supera la capacidad disponible.

Todas las redes tienen recursos limitados. Por esta razón, las redes necesitan mecanismos de QoS. La capacidad de proporcionar QoS depende de la clasificación del tráfico y de la prioridad asignada.

Clasificación

Antes de asignar estrategias de QoS, es necesario clasificar las aplicaciones según los requisitos específicos de entrega. La clasificación de datos en el origen o cerca del mismo permite asignar a dichos datos la prioridad adecuada a medida que se trasladan a través de toda la red. La segregación en clases del tráfico con características similares y luego la identificación de dicho tráfico mediante marcas es una función de los dispositivos de red en las capas de distribución y de acceso. Un ejemplo de esta estrategia es colocar el tráfico de voz de un switch de acceso en una única VLAN. Luego, el dispositivo marca el tráfico que se origina desde la VLAN de voz con la máxima prioridad.

1.4.5 Seguridad en el extremo de la red

Riesgos de seguridad en la capa de acceso

Refiera a la **Figura** del curso en línea

Muchos de los riesgos de seguridad que se producen en la capa de acceso de la red son el resultado de dispositivos finales con seguridad deficiente. Los descuidos y errores de usuario dan cuenta de la cantidad significativa de rupturas en la seguridad de la red.

¿De qué manera el diseñador de red puede mejorar la seguridad?

Quizá no esté en el alcance del proyecto de diseño de red proporcionar la seguridad adecuada para los dispositivos finales. No obstante, el diseñador necesita entender el impacto en la red que

genera un incidente de seguridad, como un gusano o un troyano, en un dispositivo final. Por lo tanto, el diseñador puede determinar mejor qué medidas de seguridad de red debe aplicar para limitar los efectos sobre la red.

Al permitir que accedan a la red sólo los dispositivos autenticados o conocidos se limita la capacidad de los intrusos de ingresar a la red. Es importante aplicar medidas de seguridad inalámbricas que cumplan con las prácticas recomendadas.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar el sitio SANS para identificar amenazas a la seguridad en Internet.

1.4.6 Medidas de seguridad

Provisión de seguridad física

Refiera a la **Figura** del curso en línea

La seguridad física de una red es muy importante. La mayoría de los intrusos de la red obtienen acceso físico en la capa de acceso. En algunos dispositivos de red, como los routers y switches, el acceso físico puede permitir cambiar contraseñas y obtener acceso total a los dispositivos.

Las medidas evidentes, como cerrar con llave los armarios de cableado y restringir el acceso a los dispositivos de red, a menudo son las formas más efectivas de prevenir rupturas de seguridad. En áreas de fácil acceso o de alto riesgo, quizá sea necesario equipar los armarios de cableado con seguridad adicional, como cámaras o alarmas y dispositivos de detección de movimiento. Algunos dispositivos, como los bloqueos de teclado, pueden registrar qué códigos se utilizan para ingresar a las áreas seguras.

Seguridad de los dispositivos de red en la capa de acceso

Las siguientes medidas simples pueden proporcionar seguridad adicional a los dispositivos de red en la capa de acceso:

- Configurar contraseñas seguras
- Utilizar SSH para administrar dispositivos
- Deshabilitar puertos sin utilizar

La seguridad de puerto del switch y el ***control de acceso a la red*** pueden asegurar que sólo los dispositivos confiables y conocidos tengan acceso a la red.

Práctica recomendada para la seguridad

Los riesgos de seguridad no pueden eliminarse o prevenirse por completo. Una efectiva evaluación y administración de riesgos puede reducir de manera considerable los riesgos de seguridad existentes. Al considerar las medidas de seguridad, es importante entender que ningún producto puede garantizar la seguridad de una organización. La verdadera seguridad de la red surge de una combinación de productos, servicios y procedimientos, junto con una cuidadosa ***política de seguridad*** y el compromiso para adherirse a esa política.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Aprender los riesgos de permitir el acceso físico a la red a personas no autorizadas.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Implementar la seguridad de puerto para evitar el acceso no autorizado.

1.5 Investigación de las granjas de servidores y la seguridad

1.5.1 ¿Qué es una granja de servidores?

Refiera a la **Figura** del curso en línea

La mayoría de las redes empresariales proporcionan a los usuarios servicios accesibles por Internet, como el correo electrónico y el e-commerce. La disponibilidad y seguridad de estos servicios es esencial para el éxito de una empresa.

Granjas de servidores

Es difícil administrar y asegurar una gran cantidad de servidores distribuidos en diferentes ubicaciones dentro de una red empresarial. La práctica recomendada centraliza los servidores en ***granjas de servidores***. Las granjas de servidores generalmente se ubican en salas informáticas y ***centros de datos***.

La creación de una granja de servidores ofrece los siguientes beneficios:

- El tráfico de la red entra y sale de la granja de servidores en un punto definido. Esta configuración facilita la seguridad, el filtrado y la priorización del tráfico.
- Los enlaces redundantes de alta capacidad pueden instalarse en los servidores y entre la red de granja de servidores y la LAN principal. Esta configuración resulta más económica que intentar proporcionar un nivel similar de conectividad a los servidores distribuidos en toda la red.
- Se puede proporcionar el ***balanceo de carga*** y la ***migración en caso de fallos*** entre los servidores y entre los dispositivos de red.
- Al disminuir la cantidad de switches de alta capacidad y de dispositivos de seguridad, se reduce el costo por la prestación de servicios.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Observar y registrar la forma en la que se traslada el tráfico desde y hacia los servidores de la red.

1.5.2 Seguridad, firewalls y DMZ

Refiera a la **Figura** del curso en línea

Los servidores del centro de datos pueden ser blanco de ataques malintencionados y deben protegerse.

Los ataques contra las granjas de servidores pueden originar una pérdidas económicas para las aplicaciones interempresariales y de e-commerce, además de generar robos de información. Deben protegerse tanto las redes de área local (LAN, local area network) como las redes de área de almacenamiento (***SAN***, storage area network) para reducir las posibilidades de que ocurran dichos ataques. Los piratas informáticos utilizan diferentes herramientas para inspeccionar las redes e iniciar ataques de intrusión y de denegación de servicio (***DoS***, denial of service).

Protección del conjunto de servidores contra ataques

Los firewalls a menudo se emplean para proporcionar un nivel básico de seguridad cuando los usuarios externos e internos intentan acceder a Internet a través de la granja de servidores. Se debe aplicar un método más exhaustivo para asegurar de manera adecuada las granjas de servidores. Este tipo de método aprovecha las ventajas de los siguientes productos de red que pueden utilizarse en una granja de servidores:

- Firewalls
- Características de seguridad del switch de la LAN

- Sistemas de prevención y detección de intrusión basados en la red y en el host
- Balanceadores de carga
- Análisis de la red y dispositivos de administración

Refiera a la **Figura** del curso en línea

Zonas desmilitarizadas

En el diseño tradicional de firewall de red, los servidores a los que se accedía desde redes externas se ubicaban en la zona desmilitarizada (***DMZ***, demilitarized zone). A los usuarios que accedían a estos servidores desde Internet o desde otras redes externas poco confiables se les impedía ver los recursos ubicados en la LAN interna. Los usuarios de la LAN eran considerados usuarios confiables y generalmente tenían pocas restricciones cuando accedían a los servidores en una DMZ.

Protección contra ataques internos

Actualmente, los ataques que se originan en la red interna son más comunes que los ataques desde fuentes externas. Como resultado, el diseño de seguridad de un conjunto de servidores es diferente del modelo DMZ anterior. Se requiere una capa de funciones de firewall y protección de intrusión entre los servidores y las redes internas; y entre los servidores y los usuarios externos. Posiblemente también sea necesario una capa de seguridad adicional entre los servidores.

La vulnerabilidad de los datos almacenados en los servidores e incluidos en las transacciones a través de la red determina la política de seguridad adecuada para el diseño de la granja de servidores.

1.5.3 Alta disponibilidad

Provisión de alta disponibilidad

Refiera a la **Figura** del curso en línea

Además de brindar una capa de seguridad adicional, generalmente es necesario que las granjas de servidores proporcionen una disponibilidad alta para los servicios y aplicaciones de red. Una red de alta disponibilidad es aquella que elimina o reduce el impacto potencial de fallas. Esta protección permite a la red cumplir con los requisitos de acceso a las aplicaciones, a los sistemas y a los datos desde cualquier lugar, en todo momento.

Creación de redundancia

Para alcanzar la alta disponibilidad, los servidores se conectan de manera redundante a dos switches separados en la capa de acceso. Esta redundancia proporciona una ruta desde el servidor hasta el switch secundario en caso de que falle el switch principal. Los dispositivos en las capas núcleo y de distribución de la red de la granja de servidores también están conectados en forma redundante. Los ***Protocolos Spanning Tree***, al igual que el Protocolo rápido de árbol de expansión (***RSTP+***, Rapid Spanning Tree Protocol), administran los enlaces redundantes de Capa 2. El Protocolo de router en espera activa (HSRP, Hot Standby Router Protocol) y los protocolos de enrutamiento proporcionan respaldo para la migración en caso de fallos y la redundancia de Capa 3.

Virtualización

Muchos de los servidores lógicos individuales pueden ubicarse en un servidor físico. El servidor físico utiliza un sistema operativo diseñado específicamente para admitir varias imágenes virtuales. Esta función se conoce como virtualización. Esta tecnología reduce el costo en la prestación de servicios redundantes, balanceo de carga y migración en caso de fallos para servicios de red esenciales.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Configurar enlaces de switch redundantes en una granja de servidores y observar lo que ocurre cuando falla un dispositivo.

1.6 Investigación de las consideraciones de red inalámbrica

1.6.1 Consideraciones exclusivas para la WLAN

Cómo comprender los requisitos del cliente

Refiera a la **Figura** del curso en línea

Antes de diseñar una implementación de LAN inalámbrica interior (***WLAN***, wireless LAN), el diseñador de red necesita entender por completo de qué manera pretende el cliente utilizar la red inalámbrica.

El diseñador aprende sobre los requisitos de red al formular preguntas al cliente. Las respuestas a estas preguntas afectan la manera en que se implementa una red inalámbrica. Los ejemplos de algunas de estas preguntas son:

- ¿Se requerirá servicio de roaming inalámbrico?
- ¿Qué autenticación de usuarios se necesita?
- ¿Se brindará acceso libre (zonas activas) a los visitantes?
- ¿Qué aplicaciones y servicios de red se encuentran disponibles para los usuarios inalámbricos?
- ¿Qué técnica de encriptación se puede utilizar?
- ¿Están planificados los teléfonos IP inalámbricos?
- ¿Qué áreas de cobertura deben respaldarse?
- ¿Cuántos usuarios hay en cada área de cobertura?

Si el diseñador no obtiene respuestas a las preguntas o no entiende por completo los requisitos del cliente, puede resultar difícil, incluso imposible, implementar una LAN inalámbrica. Por ejemplo, los requisitos para proporcionar zonas activas no protegidas son mucho menos complejos para el diseño que el acceso autenticado a los servidores internos protegidos.

Refiera a la **Figura** del curso en línea

Diseño físico de la red

En los diseños típicos de red inalámbrica, la mayor parte del esfuerzo se concentra en las áreas de cobertura física de la red.

El diseñador de red lleva a cabo un relevamiento del sitio a fin de determinar las áreas de cobertura para la red y encontrar ubicaciones óptimas para establecer puntos de acceso inalámbrico. Los resultados del relevamiento del sitio permiten determinar el hardware del punto de acceso, los tipos de antenas y los conjuntos de funciones inalámbricas deseadas. El diseñador determina si se puede admitir el servicio de roaming entre las áreas de cobertura superpuestas.

Diseño lógico de la red

Por lo general, el diseño lógico de la red es la tarea más difícil de los diseñadores de red. Los clientes a menudo desean proporcionar diferentes niveles de acceso a distintos tipos de usuarios inalámbricos. Además, las redes inalámbricas deben ser seguras y fáciles de usar. La determinación de las funciones deseadas y las limitaciones implica diferentes maneras de diseñar y configurar las LAN inalámbricas.

Un ejemplo de un diseño complejo de red inalámbrica sería una empresa que necesita ofrecer los siguientes servicios:

- Acceso inalámbrico libre para visitantes y proveedores
- Acceso inalámbrico seguro para sus empleados móviles
- Conectividad confiable para teléfonos IP inalámbricos

1.6.2 Consideraciones exclusivas para la WLAN

Refiera a la **Figura** del curso en línea

Cada tipo de acceso inalámbrico requiere de consideraciones de diseño exclusivas.

Acceso libre para visitantes

Cuando los visitantes y proveedores se encuentran en un sitio de la empresa, a menudo obtienen acceso a los sitios Web y correos electrónicos. Este tipo de acceso debe ser práctico de utilizar y generalmente no está encriptado mediante la privacidad equivalente por cable (***WEP***, Wired Equivalent Privacy) o el acceso protegido Wifi (***WPA***, Wi-Fi Protected Access). Para permitir a los usuarios visitantes conectarse a la red, se transmite el identificador del servicio (***SSID***, service set identifier) del punto de acceso.

Muchos sistemas para visitantes de zonas activas utilizan DHCP y un servidor de conexión para registrar el uso inalámbrico. Los usuarios visitantes generalmente acceden a la red inalámbrica de la siguiente manera: abren una ventana del explorador y aceptan una política de uso determinada. El sistema de registro de visitantes documenta la información del usuario y la dirección de hardware, y luego comienza a conectar el tráfico IP. Estos sistemas requieren la instalación de un servidor de aplicación en la misma red o VLAN como puntos de acceso.

Acceso seguro del empleado

Algunos dispositivos WLAN no admiten el acceso aislado para visitantes. Para asegurar el acceso del empleado, utilice una infraestructura WLAN completamente separada que no incluya el acceso para visitantes. Se recomienda separar los usuarios internos en una VLAN diferente.

Entre otras prácticas recomendadas de implementación inalámbrica se incluyen:

- SSID sin broadcast
- Encriptación segura
- Autenticación de usuario
- Tunneling de red privada virtual (***VPN***, Virtual Private Network) para datos vulnerables
- Firewall y prevención de intrusión

En áreas donde se restringe el acceso inalámbrico seguro a algunos dispositivos, se puede utilizar el filtrado de direcciones MAC para limitar el acceso.

1.7 Soporte de las WAN y los trabajadores remotos

1.7.1 Consideraciones de diseño en el margen empresarial

Refiera a la **Figura** del curso en línea

El margen empresarial es el área donde la red empresarial se conecta a redes externas. Los routers en el margen empresarial proporcionan conectividad entre la infraestructura interna del campus e In-

ternet. También proporcionan conectividad a los servicios y usuarios remotos de la WAN. Los requisitos de diseño en el margen empresarial son distintos a los requisitos dentro de la red del campus.

Costo del ancho de banda

La mayoría de las redes del campus se basan en la tecnología Ethernet. Sin embargo, la conectividad WAN en el margen empresarial generalmente se alquila de un proveedor externo que presta servicios de telecomunicaciones. El ancho de banda disponible para las conexiones WAN a menudo es considerablemente menor que el ancho de banda disponible en la LAN ya que estos servicios arrendados pueden ser costosos.

QoS

La diferencia de ancho de banda entre la LAN y la WAN puede crear cuellos de botella. Los routers extremos producen colas de datos debido a estos cuellos de botella. La previsión y administración de las colas de datos requieren de una estrategia de calidad de servicio (QoS, Quality of Service). Como resultado, el diseño y la implementación de los enlaces WAN pueden ser complicados.

Seguridad

Los requisitos de seguridad en el margen empresarial son esenciales ya que no siempre se conoce a los usuarios y servicios a los que se accede a través de los routers extremos. Se debe implementar una detección de intrusión y una inspección de firewall con estado a fin de proteger la red interna del campus ante posibles amenazas.

Acceso remoto

En muchos casos, los servicios LAN del campus deben extenderse a los trabajadores y a las oficinas remotas a través del margen empresarial. Este tipo de acceso posee requisitos distintos al nivel de acceso público proporcionado a los usuarios que ingresan a la LAN desde Internet.

1.7.2 Integración de los sitios remotos en el diseño de red

Refiera a la **Figura** del curso en línea

Al diseñar una red que admita sucursales y trabajadores remotos, es necesario que el diseñador de red se familiarice con las capacidades de las diferentes tecnologías WAN. Entre las tecnologías WAN tradicionales se incluyen:

- Líneas arrendadas
- Redes de conmutación por circuitos
- Redes de conmutación por paquete, como las redes Frame Relay
- ***Redes de conmutación por celdas***, como las redes de Modo de transferencia asíncrona (***ATM***, Asynchronous Transfer Model.)

En muchas ubicaciones se encuentran disponibles las tecnologías WAN más actuales, por ejemplo:

- Línea de suscriptor digital (DSL)
- Red Metro Ethernet
- Módem por cable
- Servicio inalámbrico de largo alcance
- Conmutación por etiquetas multiprotocolo (MPLS, Multiprotocol Label Switching)

La mayoría de las tecnologías WAN se alquilan mensualmente de un proveedor de servicios de telecomunicaciones. Según la distancia, este tipo de conectividad puede ser bastante costosa. Los

contratos WAN a menudo incluyen acuerdos del nivel de servicio (***SLA***, service level agreements). Estos acuerdos garantizan el nivel de servicio que el proveedor ofrece. Los SLA admiten aplicaciones esenciales de negocios, como por ejemplo el procesamiento de transacciones de alta velocidad y telefonía IP para ubicaciones remotas.

Refiera a la **Figura** del curso en línea

En muchas empresas, no todos los empleados trabajan en las instalaciones principales. Entre los empleados que trabajan fuera de las instalaciones se incluyen:

- Trabajadores remotos
- Trabajadores móviles
- Empleados de sucursal

Trabajadores remotos que por lo general trabajan uno o más días a la semana desde su hogar u otro lugar. Los trabajadores móviles posiblemente deben viajar constantemente a diferentes lugares o estar disponibles en forma permanente en un sitio del cliente. Algunos trabajadores son empleados de sucursales pequeñas. De cualquier forma, estos empleados necesitan tener conectividad con la red empresarial. Con el crecimiento de Internet, las empresas han recurrido a dicho servicio como medio para extender sus propias redes.

Redes privadas virtuales

Una opción de conectividad muy común, especialmente para los trabajadores remotos, es la red privada virtual (***VPN***, Virtual Private Network) a través de Internet. Una VPN es una red privada que utiliza una red pública para conectar sitios remotos o usuarios entre sí. En lugar de utilizar una conexión real dedicada, como las líneas arrendadas, una VPN utiliza conexiones virtuales enrutadas a través de Internet desde la red privada de la compañía hasta el router remoto o PC.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Colocar el cursor sobre las fotos para ver información específica del trabajador remoto. Arrastre el tipo de conexión hacia el trabajador remoto correspondiente y luego haga clic en Verificar.

1.7.3 Enlaces de respaldo y redundancia

Refiera a la **Figura** del curso en línea

Enlaces redundantes

Es necesario establecer una redundancia en enlaces WAN y es fundamental asegurar una conectividad confiable con los usuarios y sitios remotos.

Algunas aplicaciones de negocios requieren la entrega a tiempo de todos los paquetes. Para estas aplicaciones, la conectividad interrumpida no es una opción. Al proporcionar redundancia en la WAN y a través de toda la internetwork, se asegura una alta disponibilidad para las aplicaciones de extremo a extremo.

Para una WAN, los enlaces de respaldo proporcionan la redundancia necesaria. Los enlaces de respaldo a menudo utilizan tecnologías diferentes de las de la conexión primaria. Este método asegura que la falla producida en un sistema no afecte necesariamente el sistema de respaldo.

Por ejemplo, una empresa que utiliza conexiones WAN punto a punto con los sitios remotos puede utilizar las VLAN a través de Internet como una estrategia alternativa para la redundancia. DSL, ISDN y los módems dial-up son otras opciones de conectividad que se usan para proporcionar enlaces de respaldo en caso que surja una falla en la WAN. Si bien los enlaces de respaldo son a

menudo más lentos que las conexiones principales, éstos pueden configurarse para enviar solamente transacciones y datos de alta prioridad.

Carga compartida

Además de proporcionar una estrategia de respaldo, las conexiones WAN redundantes pueden proporcionar ancho de banda adicional a través de la carga compartida. El enlace de respaldo puede configurarse para proporcionar ancho de banda adicional en todo momento o sólo durante las horas pico de tráfico.

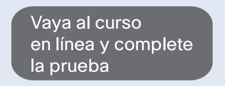
Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastrar la opción de conectividad hasta la nube correspondiente para cada ubicación de la red.

Resumen del capítulo

Examen del capítulo



Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 2

Recopilación de requisitos de red

Introducción

2.1 Presentación de Lifecycle Services de Cisco

2.1.1 El ciclo de vida de una red

Refiera a la **Figura** del curso en línea

El mundo de los sistemas de redes está evolucionando. Los sistemas de redes ya no se tratan sólo de conectar computadoras. Ahora son inteligentes y juegan un papel fundamental al contribuir a mejorar el rendimiento empresarial. Las empresas están ansiosas por expandir sus redes. Al aprovechar los avances de la tecnología, las empresas pueden agregar nuevos servicios y aumentar la productividad.

Lifecycle Services de Cisco

Lifecycle Services de Cisco está diseñado para respaldar redes en evolución. Lifecycle Services de Cisco es un enfoque de seis fases. Cada fase define las actividades necesarias para operar e implementar exitosamente las tecnologías de Cisco. También describe cómo optimizar el rendimiento durante el ciclo de vida de una red.

Las seis fases del Lifecycle Services de Cisco son:

- Fase de preparación
- Fase de planificación
- Fase de diseño
- Fase de implementación
- Fase de operación
- Fase de optimización

Este proceso generalmente se denomina ***PPDIOO***, según las primeras letras de cada una de las seis fases.

Refiera a la **Figura** del curso en línea

Estudio de caso: Red del estadio deportivo

La organización administrativa de un estadio está trabajando con CompañíadeRedes para renovar y actualizar la red del estadio. La red del estadio ha crecido año tras año. Sin embargo, no se han considerado en gran medida el diseño de la infraestructura ni los objetivos empresariales generales. Se ha seguido adelante con algunos proyectos nuevos. Sin embargo, los administradores de red no tenían un conocimiento real del ancho de banda, la prioridad del tráfico ni otros requisitos necesarios para respaldar un tipo de red avanzada y esencial para la empresa. La administración del estadio actualmente desea agregar nuevas funciones de alta tecnología, pero la red existente no es capaz de admitirlas.

Fases del ciclo de vida de la red

Los representantes de CompañíadeRedes se reúnen con la administración del estadio para analizar el proceso que intentan utilizar para diseñar la nueva red. Si bien la fase de diseño es sólo una de las fases en el ciclo de vida de la red, todas las fases del PPDIOO afectan las decisiones de diseño.

Durante las fases de preparación y planificación, el diseñador de red y el personal del estadio identifican los objetivos empresariales y requisitos técnicos de la organización del estadio, además de cualquier limitación en el diseño. Esta recopilación de requisitos que se produce durante estas fases influye en las decisiones tomadas durante la fase de diseño.

La fase de implementación comienza luego de aprobar el diseño. Se incluye la integración inicial del nuevo diseño en la red existente.

Durante las fases de optimización y operación, el personal del estadio analiza y monitorea el rendimiento de la red.

2.1.2 Fase de preparación del ciclo de vida de la red

Fase de preparación

Refiera a la **Figura** del curso en línea

Durante la fase de preparación, la administración del estadio y el personal de CompañíadeRedes definen los siguientes objetivos empresariales:

- Mejorar la experiencia del cliente
- Reducir los costos
- Agregar servicios adicionales
- Respaldar la expansión de la compañía

Estos objetivos sirven de base para el ***caso comercial***. El caso comercial se utiliza para justificar la inversión financiera necesaria para implementar el cambio tecnológico. La compañía considera las posibles limitaciones empresariales que incluyen el presupuesto, el personal, las políticas de la compañía y las limitaciones en el cronograma.

Una vez aceptado el caso comercial, el personal de CompañíadeRedes contribuye al desarrollo de soluciones y estrategias tecnológicas de alto nivel.

Esta estrategia identifica lo siguiente:

- Tecnologías avanzadas que respaldan la nueva solución de red
- Aplicaciones y servicios de red actuales y planificados, y sus prioridades según los objetivos empresariales
- Personas, procesos y herramientas necesarias para respaldar las operaciones y la administración de la solución tecnológica

La fase de preparación generalmente se realiza antes de que la compañía emita una Solicitud de propuesta (***RFP***, Request For Proposal) o una Solicitud de presupuesto (***RFQ***, Request For Quotation). Las RFP y RFQ describen los requisitos para la nueva red. Éstas incluyen información sobre el proceso que la compañía utiliza para comprar e instalar tecnologías de sistemas de red.

2.1.3 Fase de planificación del ciclo de vida de la red

Fase de planificación

Refiera a la **Figura** del curso en línea

Durante la fase de planificación, el diseñador de red realiza una evaluación integral del sitio y de las operaciones. En esta evaluación se analiza la red, las operaciones y la infraestructura administrativa de la red actuales.

El personal de CompañíadeRedes identifica todas las modificaciones eléctricas, ambientales y físicas. También evalúa la capacidad que tienen las operaciones actuales y la infraestructura administrativa de la red para respaldar la nueva solución tecnológica. Todos los cambios de infraestructura, personal, procesos y herramientas deben completarse antes de implementar la nueva solución tecnológica.

También se identifican en esta fase las aplicaciones personalizadas que se agregan a los requisitos en torno a las características y la funcionalidad para la nueva red. El personal de CompañíadeRedes crea un documento que contiene todos los requisitos de diseño.

Plan de proyecto

En esta fase, el personal de CompañíadeRedes y la administración del estadio crean un plan para contribuir a la administración del proyecto. El plan del proyecto incluye:

- Tareas
- Cronogramas e hitos importantes
- Riesgos y limitaciones
- Responsabilidades
- Recursos necesarios

El plan debe incluirse dentro de los límites de recurso, costo y alcance establecidos en los objetivos empresariales originales. La administración del estadio y CompañíadeRedes asignan personas para administrar el proyecto.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

A partir de la información suministrada, identificar las limitaciones y los objetivos empresariales para CompañíaCinematográfica.

2.1.4 Fase de diseño del ciclo de vida de la red

Fase de diseño

Refiera a la **Figura** del curso en línea

En la fase de diseño, el personal de CompañíadeRedes utiliza los requisitos iniciales establecidos durante la fase de planificación para dirigir su trabajo.

El documento sobre requisitos de diseño respalda las especificaciones identificadas en las fases de planificación y preparación para lo siguiente:

- ***Disponibilidad***
- ***Escalabilidad***
- ***Seguridad***
- ***Facilidad de administración***

El diseño debe ser lo suficientemente flexible como para permitir cambios o adiciones a medida que surgen nuevas necesidades u objetivos. La tecnología debe integrarse en la infraestructura administrativa de la red y en las operaciones actuales.

Planificación de la instalación

Al finalizar la fase de diseño, el diseñador de red crea planes que guían la instalación y aseguran que el resultado final cumpla con los requisitos del cliente. Los planes incluyen:

- Configurar y probar la conectividad
- Implementar el sistema propuesto
- Demostrar la funcionalidad de la red
- Migración de las aplicaciones de la red
- Validar el funcionamiento de la red
- Capacitar a los usuarios finales y al personal de soporte

El diseño de la red se completa durante la fase de diseño en la actualización de la red del estadio. Se especifican y prueban los nuevos equipos y tecnologías. Al revisar el diseño propuesto se confirma si los objetivos empresariales se han cumplido. Se elabora una propuesta final para continuar con la implementación de la actualización de la red.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

MCSA: redacte tres o cuatro preguntas sobre las fases de diseño, planificación y preparación.

2.1.5 Fase de implementación del ciclo de vida de la red

Fase de implementación

Refiera a la **Figura** del curso en línea

La fase de implementación comienza una vez que CompañíadeRedes completa el diseño y el cliente lo aprueba. La red se crea según la especificación de diseño autorizada. La fase de implementación verifica el éxito o fracaso del diseño de red.

Prueba de la nueva red

La prueba de una parte o de toda la solución de la nueva red en un entorno controlado permite identificar y resolver cualquier problema de implementación antes de realizar la instalación en sí.

Luego de haber resuelto los problemas, el personal de CompañíadeRedes instala la nueva solución y la integra a la red existente. Se realiza una prueba adicional al terminar la instalación.

La ***prueba de aceptación de nivel de sistema*** verifica que la nueva red cumpla con los objetivos empresariales y los requisitos de diseño. Los resultados de esta prueba se registran y se incluyen en la documentación suministrada al cliente. Es necesario completar cualquier capacitación requerida para el personal del estadio durante esta fase.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastre el término hacia la definición correcta y luego haga clic en Verificar.

2.1.6 Fase de operación del ciclo de vida de la red

La fase de operación

Refiera a la **Figura** del curso en línea

Las fases de operación y optimización son procesos continuos. Éstas representan las operaciones cotidianas de una red. El personal del estadio monitorea la red y establece una ***línea de base de red***. Este monitoreo permite a la compañía alcanzar la máxima escalabilidad, disponibilidad, seguridad y facilidad de administración.

Luego de instalar la nueva red, el personal del estadio administra dicha red para asegurarse de que funcione según las especificaciones de diseño descritas en las fases de planificación y preparación.

Definición de políticas y procedimientos

Las políticas y los procedimientos son necesarios para tratar aspectos de la red, por ejemplo:

- Incidentes de seguridad
- Cambios de configuración
- Compras de equipo

La actualización de estas políticas y procedimientos luego de una mejora reduce el tiempo de inactividad, los costos operativos y cuestiones relacionadas con cambios. Si no existen políticas ni procedimientos vigentes, es importante crearlos.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar el Asistente de Cisco Network para observar el tráfico.

2.1.7 Fase de optimización del ciclo de vida de la red

Fase de optimización

Refiera a la **Figura** del curso en línea

La optimización de la red es un proceso continuo. El propósito de esta fase es mejorar el rendimiento y la confiabilidad de la red al identificar y resolver posibles problemas de red antes de que ocurran. Mediante este proceso se asegura el mantenimiento de los requisitos y objetivos empresariales de la compañía. Entre los problemas comunes de red que pueden detectarse en la fase de optimización se incluyen:

- Incompatibilidad de funciones
- Capacidad de enlace insuficiente
- Problemas con el rendimiento de los dispositivos cuando se habilitan múltiples funciones
- Escalabilidad de protocolos

A medida que cambian los objetivos empresariales, es posible que las operaciones y estrategias tecnológicas no se adapten. En algún punto, será necesario elaborar un nuevo diseño y el ciclo PPDIOO comenzará nuevamente.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Para cada acción mencionada a la izquierda, coloque una marca en la columna de la fase de preparación, planificación, diseño, implementación, operación U optimización y después haga clic en Verificar.

2.2 Descripción del proceso de ventas

2.2.1 Respuesta a una solicitud de propuesta o presupuesto del cliente

Refiera a la **Figura** del curso en línea

Cuando una empresa u organización decide actualizar o reemplazar su red actual, ésta a menudo genera una Solicitud de propuesta (RFP) o una Solicitud de presupuesto (RFQ). En el modelo PPDIOO, esto sucede al final de la fase de preparación. Las RFP y RFQ incluyen especificaciones que definen el formato y contenido de las respuestas que se esperan de los posibles contratistas. Es fundamental que los contratistas cumplan con las instrucciones establecidas en el documento con la mayor precisión posible. El incumplimiento de las directivas o la omisión de secciones de la solicitud, puede provocar que el proyecto se asigne a otro contratista.

Además del contenido y formato de la respuesta, las RFP y RFQ incluyen cronogramas que deben cumplirse. La compañía que ha enviado la RFP puede rechazar una respuesta tardía.

Respuesta a la solicitud

Cada sección del documento de respuesta debe ser lo más detallado posible. Los números de sección del documento de respuesta deben coincidir con los números de sección de la solicitud, a menos que se indique lo contrario. La respuesta debe redactarse teniendo en cuenta la audiencia a la que va dirigida. Se deben explicar conceptos y términos técnicos cuando sea necesario.

Para asegurar que el documento de respuesta sea fácil de leer, se utiliza un índice para organizar el material. Se incluye una carta de presentación para introducir el material.

2.2.2 Asistencia a la reunión previa a la oferta

Reunión previa a la oferta

Refiera a la **Figura** del curso en línea

Antes del plazo para presentar respuestas a la RFP, el cliente puede programar una reunión informativa. Esta reunión puede denominarse reunión previa a la oferta o conferencia previa a la propuesta. El propósito de esta reunión es ofrecer lo siguiente:

- Una oportunidad para revisar con el cliente el alcance del proyecto
- Documentación e información adicional que se identifica pero no se incluye en la RFP original
- Aclaración de los detalles de formato y cronograma del proyecto que no se incluyen en la RFP original

La reunión permite al contratista obtener un cálculo de la cantidad de compañías interesadas en presentar una oferta para el proyecto. Si no se programa una reunión previa a la oferta, la información o documentación puede solicitarse directamente al personal adecuado que se indica en la RFP.

2.2.3 Explicación de la Solicitud de propuesta (RFP)

Solicitud de propuesta

Refiera a la **Figura** del curso en línea

Las empresas que publican una RFP generalmente envían una copia de la RFP a los contratistas. De vez en cuando, las RFP pueden publicarse en el sitio Web de la empresa. Las respuestas a una RFP permiten al cliente comparar servicios, productos, precios y soporte que ofrecen distintos contratistas.

Por lo general, la RFP para un proyecto de red incluye:

Refiera a la **Figura** del curso en línea

- Objetivos empresariales del proyecto
- Alcance previsto del proyecto
- Información sobre la red y las aplicaciones actuales
- Requisitos para la nueva red
- Limitaciones empresariales, técnicas o ambientales
- Programa preliminar con hitos y entregas
- Términos y condiciones legales del contrato

Al responder una RFP, es importante contestar cada punto mencionado en la RFP. La compañía que ha enviado la RFP puede rechazar una propuesta incompleta.

2.2.4 Explicación de la Solicitud de presupuesto (RFQ)

Solicitud de presupuesto

Refiera a la **Figura** del curso en línea

Las empresas que publican una RFQ utilizan una RFQ en lugar de una RFP cuando ya se conocen las especificaciones técnicas del proyecto. Si una empresa cuenta con un personal de soporte de red capacitado, éste puede redactar una RFQ para obtener los costos de los equipos y servicios necesarios. Una RFQ por lo general es mucho más simple de responder que una RFP ya que los costos asociados con una RFQ pueden calcularse u obtenerse fácilmente.

Una RFQ puede variar en contenido pero generalmente incluye tres partes principales. Al igual que una RFP, la respuesta a una RFQ puede incluir varios requisitos de formato. El cumplimiento de los plazos de la propuesta puede exigirse de manera estricta.

Para responder una RFQ deben cumplirse las mismas pautas utilizadas al responder una RFP. Cumpla de manera precisa con todas las directivas y presente la respuesta antes del plazo para asegurar su consideración.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastre el elemento de la derecha hacia la parte correspondiente de la RFQ y luego haga clic en Verificar.

2.2.5 Explicación del rol de un gerente de cuentas

Refiera a la **Figura** del curso en línea

Cuando CompañíadeRedes recibe la RFP de Compañía Estadio, la tarea de responder se le asigna a un gerente de cuentas. Los gerentes de cuentas de CompañíadeRedes son responsables de mantener una relación continua entre la compañía y sus clientes. Esta relación comienza cuando un gerente de cuentas se comunica primero con un posible cliente. Luego continúa durante todas las fases del ciclo de vida PPDIOO de la red. Los clientes de la empresa confían en que el conocimiento y la experiencia de su gerente de cuentas les ayudará a determinar los requisitos de la red. Es fundamental ganar y mantener la confianza del cliente para el éxito de un gerente de cuentas. El gerente de cuentas asignado a la cuenta del estadio es responsable de asegurar una relación comercial óptima entre Compañía Estadio y CompañíadeRedes.

Canal de comunicaciones

El gerente de cuentas actúa como contacto principal de CompañíadeRedes para el personal administrativo del estadio. Un gerente de cuentas eficiente necesita contar con excelentes habilidades interpersonales y un conocimiento completo del negocio del cliente. El gerente de cuentas se comunica con la administración del estadio mediante reuniones en persona, llamadas telefónicas, correos electrónicos o una combinación de más de un método, según las preferencias del cliente.

Refiera a la **Figura** del curso en línea

Responsabilidades del gerente de cuentas

En algunas compañías, los gerentes de cuentas son responsables de contactar a todos los clientes actuales y potenciales dentro de un territorio o área geográfica. Otras compañías asignan cuentas a estos gerentes según el tipo de negocio del cliente. Si bien las tareas específicas pueden variar según el cargo, la mayoría de los gerentes de cuentas son responsables de:

- Cumplir con sus objetivos de ganancia y venta asignados
- Comunicar información sobre tecnologías o productos nuevos a los clientes actuales y potenciales
- Dirigir ventas locales, servicios y equipos de soporte
- Planificar y elaborar un presupuesto para proyectos de soporte y ventas
- Responder a las solicitudes del cliente sobre propuestas, demostraciones, presupuestos e información
- Negociar y mantener contratos de servicio o ventas

En CompañíadeRedes, es necesario que los gerentes de cuenta obtengan capacitación sobre administración de clientes y ventas, además de demostrar habilidades básicas de sistemas de redes.

2.2.6 Explicación del rol de un ingeniero preventa en sistemas

Refiera a la **Figura** del curso en línea

CompañíadeRedes emplea personal técnico de preventa y posventa para ayudar al gerente de cuentas a brindar soporte técnico a sus clientes.

Ingeniero preventa en sistemas

Los ingenieros preventa en sistemas (a menudo denominados ingenieros preventa de soporte técnico) ayudan al gerente de cuentas y al cliente a determinar la necesidad de realizar actualizaciones o incorporaciones a la red del cliente. Los gerentes de cuentas confían en la experiencia técnica de los ingenieros preventa en sistemas para asegurar que cualquier equipo o servicio nuevo sea adecuado según las necesidades de red del cliente. En las fases de diseño y planificación del ciclo de vida PPDIOO, los ingenieros preventa en sistemas brindan asistencia para determinar los requisitos técnicos y la factibilidad de los cambios propuestos para la red. Estos ingenieros, al igual que los técnicos de red que trabajan con ellos, son responsables de:

- Evaluar la red actual del cliente
- Determinar si se cumple con los requisitos técnicos al incorporar o actualizar una red
- Asegurar que los cambios propuestos puedan integrarse a la red actual del cliente
- Probar y evaluar las soluciones propuestas

El ingeniero preventa en sistemas ayuda al diseñador de red a identificar problemas con la red actual o posibles problemas que puedan provocar los cambios a la red. La identificación y resolución temprana del problema es fundamental para el éxito de una instalación o actualización de una red. El ingeniero preventa en sistemas juega un papel fundamental al crear un documento de respuesta preciso ante una RFP.

Los requisitos de capacitación para los ingenieros preventa en sistemas incluyen cursos de diseño de red al igual que cursos de tecnología de red. Muchos ingenieros preventa en sistemas deben adquirir certificaciones de diseño de red. Un ejemplo de dicha certificación sería la Cisco Certified Design Associate (CCDA).

2.2.7 Explicación del rol de un diseñador de red

Refiera a la **Figura** del curso en línea

Un diseñador de red necesita tener un conocimiento completo de las capacidades de todos los tipos de equipos y tecnologías de sistemas de red. Estas habilidades permiten al diseñador proporcionar a los clientes un diseño de red que cumpla con los requisitos del cliente en torno a la escalabilidad, disponibilidad, seguridad y facilidad de administración. El diseñador participa de las fases de diseño y planificación del ciclo de vida PPDIOO de la red. En algunas compañías más pequeñas, el ingeniero preventa en sistemas también puede desempeñar el rol de un diseñador de red. En las compañías más grandes, es posible que exista un equipo de diseñadores de red trabajando en un único proyecto. En este curso se utilizará un único diseñador de red.

Un diseñador de red eficiente dedica su tiempo a aprender sobre el negocio del cliente y sus requisitos de red. Esto permite al diseñador anticipar los cambios que pueden ocurrir a medida que la empresa crece y alcanza el éxito. Un diseñador es responsable de:

- Analizar los objetivos y limitaciones del cliente a fin de determinar los requisitos técnicos para el nuevo diseño
- Evaluar la red actual instalada
- Seleccionar las capacidades del equipo y las tecnologías para cumplir con los requisitos definidos de la red
- Diagramar la ubicación e interconexión de los diferentes servicios y dispositivos de red
- Diseñar y supervisar la prueba de concepto
- Ayudar al gerente de cuentas a preparar presentaciones para el cliente

Refiera a la **Figura** del curso en línea

En CompañíadeRedes, el personal de diseño está conformado por profesionales de red altamente capacitados. El diseñador de red debe mantenerse actualizado acerca de las tecnologías y las nuevas prácticas de diseño recomendadas.

Es necesario que el diseñador obtenga certificaciones de diseño de red, además de certificaciones profesionales técnicas sobre redes.

El diseñador al que se le asigna la actualización del estadio es un profesional con certificación CCDP (Cisco Certified Design Professional). Al obtener esta certificación avanzada, el diseñador demuestra las competencias necesarias para diseñar una red compleja para la compañía del estadio.

2.2.8 Explicación del rol de un ingeniero posventa de campo

Refiera a la **Figura** del curso en línea

Durante las fases de implementación, operación y optimización del ciclo de vida PPDIOO de la red, el ingeniero posventa de campo (a menudo denominado ingeniero posventa de soporte técnico) asume del personal de preventa la responsabilidad de ofrecer soporte técnico. Por lo general, se trata de un ingeniero posventa de campo responsable de instalar sin inconvenientes el nuevo equipo de red. Los ingenieros posventa de campo trabajan con los clientes para asegurar que la actualización de la red funcione según el diseño.

Responsabilidades de un ingeniero posventa de campo

Entre las responsabilidades de un ingeniero posventa de campo se incluyen:

- Proporcionar pruebas de aceptación y asistencia en la instalación.
- Apoyar y organizar la resolución de problemas de componentes o sistemas.

- Resolver los problemas técnicos que el cliente pueda tener.
- Proporcionar asistencia y capacitación al cliente sobre administración y configuración de dispositivos.

El ingeniero posventa de campo ayuda a desarrollar los cambios recomendados al diseño de la red a través del ciclo de vida PPDIOO.

Los requisitos de capacitación para los ingenieros posventa de campo incluyen cursos básicos y avanzados sobre tecnología de redes. En algunas tecnologías, como voz IP, es necesario que el ingeniero posventa de campo tome otros cursos de capacitación avanzados. La certificación Cisco Certified Network Associate (CCNA) se considera el requisito mínimo para la mayoría de los cargos de ingeniero posventa de campo.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastre el rol hacia la actividad correcta y luego haga clic en Verificar.

2.3 Preparación para el proceso de diseño

2.3.1 Trabajo con el cliente

Refiera a la **Figura** del curso en línea

Al diseñar la nueva red para el estadio, CompañíadeRedes interactúa con el personal de las oficinas del estadio. Cuando el diseñador de red y el personal se reúnen con el personal del estadio, es importante que se comporten de manera profesional.

Importancia de las habilidades interpersonales

Es esencial tener buenas habilidades interpersonales al interactuar con los clientes. Una actitud cordial y tranquila inspira confianza en los clientes. El cliente cree que el personal y el diseñador de CompañíadeRedes pueden realizar las tareas necesarias.

Las siguientes habilidades son esenciales al trabajar con clientes:

- Escuchar y resumir información en forma precisa
- Mantener comunicaciones con los clientes en un estilo, formato y grado de detalle adecuado para la audiencia a la que se dirige
- Presentar material técnico bien organizado de manera lógica

Es esencial la capacidad de desarrollar una buena relación de confianza mutua con el cliente. Al establecer una relación laboral de confianza, se eliminan muchos problemas potenciales y se contribuye en gran medida al éxito del proyecto para ambas compañías.

2.3.2 Definición de cliente

Refiera a la **Figura** del curso en línea

Para crear un plan integral, el diseñador de red necesita entender de qué manera los usuarios de la red interactúan con los servicios y recursos de la red. El diseñador reúne información sobre todo el acceso interno y externo a la infraestructura de la red actual. Sin un conocimiento completo de quiénes tienen acceso a la red, el diseñador puede pasar por alto algunos requisitos de usuario. Como resultado, el diseñador puede presentar un diseño incompleto. Al no presentar un diseño adecuado se generan demoras y aumentos en los costos.

Identificación de la información relevante

Al reunir información sobre la infraestructura, el diseñador trabaja con el personal del estadio para identificar a todos los grupos de usuarios. El diagrama de organización del cliente es uno de los tantos elementos que debe adquirir el diseñador. Es importante observar más allá del diagrama de organización para identificar todos los usuarios finales y personas interesadas que acceden a la red del cliente.

La administración del estadio identifica estos posibles usuarios finales:

- Personal de oficina local o sucursal
- Trabajadores remotos
- Personal de soporte y ventas que trabaja fuera del lugar de trabajo
- Vendedores, proveedores y socios
- Miembros de la junta directiva
- Asesores y contratistas
- Clientes

Incorporación de acceso a usuarios

El diseñador también necesita evaluar el impacto al agregar nuevos grupos de usuarios a la red. Algunos grupos de usuarios finales que actualmente no tienen acceso a la red posiblemente necesiten acceder a los nuevos recursos de red del estadio en el futuro.

El diseñador trabaja con la administración del estadio para identificar:

- Nuevos grupos de usuarios
- El tipo de acceso requerido
- Dónde se permite el acceso
- El impacto total en la seguridad

Al incluir esta información en las fases de preparación y planificación se puede asegurar un nuevo diseño preciso y exitoso.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear una estructura de organización de red de CompañíaCinematográfica. Incluya a todas las partes interesadas en la estructura: usuarios internos de la red, organizaciones de TI, clientes externos, proveedores y socios.

2.3.3 Identificación de prioridades y objetivos empresariales

Refiera a la **Figura** del curso en línea

El objetivo de toda empresa es alcanzar el éxito. Antes de comenzar cualquier proyecto de red, los gerentes empresariales analizan la factibilidad del proyecto según la manera en que contribuye con el éxito de la empresa. Deben considerar lo siguiente:

- Rentabilidad: ¿El proyecto puede reducir los costos o ayudar a la empresa a evitar costos en el futuro?
- Crecimiento empresarial y participación en el mercado: ¿El proyecto puede ayudar a la empresa a crecer de manera más eficiente o crear ventajas competitivas?

- Satisfacción del cliente: ¿El proyecto puede mejorar la experiencia del cliente y aumentar la lealtad de éste?

Este análisis de factibilidad permite a los gerentes empresariales reunir una lista de objetivos de alto nivel para el proyecto de red. El diseñador de red considera estos objetivos y registra cualquier problema o inquietud que se mencione.

Prioridad de los objetivos

El diseñador prioriza los objetivos empresariales al consultar con la administración del estadio. Las prioridades se basan en los objetivos que representan la mejor oportunidad de contribuir al éxito de la empresa. Por ejemplo, la importancia relativa de cada objetivo puede clasificarse como porcentaje del total de 100.

Una vez que CompañíadeRedes obtiene la lista de los objetivos empresariales en orden de prioridad, comienza la fase de planificación.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Para asegurar que la información recopilada sea precisa, cree una lista de verificación de los objetivos empresariales de CompañíaCinematográfica.

2.4 Identificación de requisitos y limitaciones técnicas

2.4.1 Definición de requisitos técnicos

Refiera a la **Figura** del curso en línea

Luego de obtener los objetivos empresariales en orden de prioridad, el diseñador de red determina la funcionalidad que la red necesita para cumplir con todos los objetivos. El diseñador menciona los objetivos empresariales que debe cumplir el nuevo diseño y luego decide lo que se necesita en términos técnicos para implementar cada cambio.

Al determinar los requisitos técnicos, el diseñador puede establecer el alcance del proyecto. Estos requisitos guían la selección de tecnologías, equipo y software de administración.

Estos requisitos técnicos incluyen, entre otros:

- Mejorar la escalabilidad de la red
- Aumentar la disponibilidad y el rendimiento de la red
- Mejorar la seguridad de la red
- Simplificar el soporte y la administración de la red

Refiera a la **Figura** del curso en línea

El diseñador de red trabaja con el cliente para crear una lista de requisitos técnicos en orden de prioridad. Esta lista representa una guía para las siguientes decisiones:

- Seleccionar el equipo de red
- Elegir los protocolos
- Diseñar servicios de red

Esta lista de proyecto define el alcance del mismo.

Al analizar los requisitos técnicos con el cliente, el diseñador considera el nivel de conocimientos técnicos de la audiencia. Es posible que el cliente no entienda con claridad la jerga y la termi-

nología técnica. Dichos términos deben evitarse o ajustarse al nivel de detalle y complejidad que pueda entender el cliente.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en laboratorio

Utilizar los objetivos empresariales de CompañíaCinematográfica para crear y priorizar los requisitos técnicos para la red.

2.4.2 Identificación de las limitaciones

Refiera a la **Figura** del curso en línea

Todas las compañías desean tener disponible la red más avanzada y eficiente. En la práctica, existen muchas limitaciones empresariales que afectan el diseño de red. Entre las limitaciones comunes se incluyen:

- ***Presupuesto:*** los recursos limitados pueden afectar el diseño debido a los costos de equipo, software u otros componentes.
- ***Políticas de la compañía:*** el diseño debe considerar las políticas actuales del cliente con respecto a los protocolos, estándares, proveedores y aplicaciones.
- ***Cronograma:*** el plazo del proyecto debe ajustarse a los horarios del cliente.
- ***Personal:*** la disponibilidad de personal capacitado en las fases de operación e implementación puede representar una consideración de diseño.

Las limitaciones realmente afectan el diseño de red y deben detectarse temprano en el proceso del ciclo de vida PPDIOO. La importancia relativa de las limitaciones varía según el proyecto. Las limitaciones en el presupuesto no son siempre la principal consideración para un proyecto grande.

Para el proyecto de red del estadio, la administración no desea programar la implementación durante su temporada deportiva.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Identificar las limitaciones para el proyecto de red de CompañíaCinematográfica.

2.5 Identificación de las consideraciones de diseño sobre facilidad de administración

2.5.1 Utilización del enfoque de diseño descendente

Refiera a la **Figura** del curso en línea

Existen dos enfoques comunes para el diseño de red: descendente y ascendente.

Descendente

El enfoque descendente adapta la infraestructura de la red a las necesidades de la organización. Este enfoque deja en claro los objetivos de diseño y lo inicia desde la perspectiva de las soluciones de red y aplicaciones requeridas, como la telefonía IP, las redes de contenido y la videoconferencia. La metodología PPDIOO utiliza un enfoque descendente.

Ascendente

Un enfoque común (pero no recomendable) es el diseño ascendente. En este enfoque, el diseñador de red selecciona las tecnologías y los dispositivos de red según la experiencia previa y no a partir del conocimiento de la organización. El diseño de red propuesto quizá no pueda admitir las aplicaciones requeridas debido a que este enfoque no incluye información sobre los objetivos empresariales.

2.5.2 Monitoreo de las operaciones de red

Refiera a la **Figura** del curso en línea

Luego de la implementación, es importante asegurar el cumplimiento de las especificaciones del diseño de red. El personal de la red del estadio monitorea y administra el rendimiento de la red. La administración de red incluye las siguientes funciones:

- Administrar los cambios de configuración en la red
- Identificar fallas en la red
- Monitorear los niveles de rendimiento
- Proporcionar administración contable y de seguridad para uso grupal e individual de la red

Una arquitectura típica de administración de red consta de los siguientes elementos:

- Sistema de administración de red (***NMS***, Network Management System): un sistema que utiliza una aplicación para monitorear y controlar los dispositivos de red administrados, como CiscoWorks
- Protocolo de administración de red: un protocolo que facilita el intercambio de información entre los dispositivos de red y NMS, como el Protocolo simple de administración de red (SNMP) versión 3 (***SNMP***v3)
- Dispositivos administrados: dispositivos de red que se administran mediante un NMS, como un router o switch
- Agentes de administración: software de dispositivos administrados que reúnen y almacenan información de administración de la red
- Información de administración: datos recopilados por el NMS

Refiera a la **Figura** del curso en línea

CiscoWorks LAN Management Solution (LMS) es un conjunto de herramientas de administración de gran utilidad que simplifican la configuración, administración, monitoreo y resolución de problemas de las redes de Cisco. Integra estas capacidades en una solución del mejor nivel que proporciona los siguientes beneficios:

- Mejora la eficiencia y precisión del personal operativo de la red
- Aumenta la disponibilidad general de la red al simplificar la configuración e identificar y resolver rápidamente problemas de red
- Maximiza la seguridad de la red a través de la integración con los servicios de control de acceso y la auditoría de los cambios a nivel de la red

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar un programa de software para monitorear el rendimiento de la red.

2.5.3 Herramientas para el monitoreo de la red

Refiera a la **Figura** del curso en línea

SNMP es el protocolo de administración de red de mayor uso. El protocolo permite que los administradores de red reúnan datos sobre la red y los dispositivos correspondientes. El software del sistema de administración SNMP se encuentra disponible en herramientas como CiscoWorks. El software del agente de administración SNMP suele estar incorporado en los sistemas operativos de servidores, routers y switches.

SNMP incluye cuatro componentes principales:

- Estación de administración
- Agentes de administración
- Base de información de administración (***MIB***, Management Information Base)
- Protocolo de administración de red

Como parte del sistema de administración de red, las herramientas de SNMP pueden responder ante errores o fallas de la red de distintas maneras. Por lo general, cuando ocurre una falla en la red, o cuando se alcanza un umbral predeterminado, las herramientas de SNMP pueden responder mediante alguna de las siguientes acciones:

- Envío de una alerta en la red
- Envío de un mensaje a un radiolocalizador
- Envío de un correo electrónico a un administrador

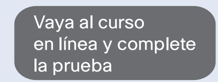
La administración del estadio necesita adquirir un software de administración de red, ya que quizá desee ofrecer acuerdos del nivel de servicio a sus proveedores.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Investigar las capacidades e informes disponibles en el software de monitoreo de red.

Resumen del capítulo



Examen del capítulo

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 3

Descripción de la red actual

Introducción

Refiera a la **Figura** del curso en línea

3.1 Documentación de la red actual

3.1.1 Creación de un diagrama de red

Refiera a la **Figura** del curso en línea

Por lo general, el primer paso para instalar una nueva red es observar detalladamente la red actual. El diseñador de CompañíadeRedes examina la red actual para:

- Determinar si los objetivos de diseño son realistas y factibles
- Determinar si la red actual cumple con las expectativas en torno a la escalabilidad, disponibilidad, seguridad y facilidad de administración
- Identificar dónde pueden integrarse los equipos, las actualizaciones de la infraestructura y los servicios nuevos
- Asegurar que las funciones, medios y dispositivos de red nuevos y antiguos puedan funcionar en conjunto

Actualización de la red del estadio

Al igual que en muchas organizaciones, el estadio cuenta con una red preexistente. La administración desea instalar una nueva red para:

- Administrar mejor las redes de datos, video y voz existentes
- Mejorar el servicio al cliente
- Reducir los costos

Refiera a la **Figura** del curso en línea

El diseñador de CompañíadeRedes revisa la documentación de la red actual. La documentación de red del departamento de TI del estadio contiene la mayor parte de la información que necesita el diseñador acerca de los servicios y la organización de la red.

La documentación de red debe incluir:

- Diagramas físicos y lógicos de la red
- Planos de piso que muestren la ubicación de los armarios para el cableado y tendidos de cables
- Listas de inventario del equipo de red instalado
- Archivos de configuración de la red actual
- Listas de inventario de las aplicaciones de red

Producción de un mapa de topología de la red

Como ocurre en muchas empresas, la documentación de red de EstadioCompañía no está actualizada. Será necesario crear un nuevo diagrama de la red en su totalidad, junto con los diferentes segmentos que abarca.

Los programas de administración de red reúnen información y producen un diagrama de la red actual. El Asistente de Cisco Network y CiscoWorks son dos ejemplos de programas de administración de red.

Refiera a la **Figura** del curso en línea

El Asistente de Cisco Network se utiliza para obtener la información necesaria para producir un diagrama de la red del estadio.

Recopilación de información sobre rutas de datos y dispositivos

El personal de CompañíadeRedes ahora puede conectarse a varios dispositivos de red. El diseñador de red utiliza los comandos estándares de IOS de Cisco para obtener información sobre los dispositivos y las rutas que los datos siguen en la red.

El software IOS de Cisco ofrece comandos útiles para obtener información de un router a fin de crear un diagrama de red. Algunos de estos comandos son:

- `show version`
- `show running-config`
- `show ip route`
- `show cdp neighbors detail`
- `show controllers`
- `show tech-support`

El comando **`show tech-support`** puede recolectar gran cantidad de información sobre un router. El resultado de este comando varía según la configuración o la plataforma del switch o router.

Muchos de estos mismos comandos se utilizan para obtener información sobre un switch de Cisco. Otros comandos útiles de switches son:

- `show vlan`
- `show vtp`
- `show spanning-tree`

Refiera al **Gráfico Interactivo** del curso en línea

Actividad personalizada de página completa

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Utilizar los comandos de switch y router para investigar los dispositivos de la red actual.

3.1.2 Diagrama de la arquitectura lógica

Luego de recolectar información sobre la red actual, la próxima tarea es crear o actualizar uno o más diagramas lógicos de la red.

Refiera a la **Figura** del curso en línea

Creación de un diagrama general de la red actual

En el proyecto de red del estadio, el primer diagrama que crea el diseñador de red consiste en un panorama de alto nivel de todos los sitios de red del estadio. El diagrama muestra:

- La red principal del estadio
- La tienda de recuerdos

- Los centros de venta de entradas
- La conectividad a los sitios remotos
- La conectividad a los socios comerciales

El diseñador diagrama las conexiones ***WAN*** entre redes y el equipo en cada ubicación donde termina la WAN.

Este diagrama de red muestra de qué manera fluye la información desde un área de la red hacia otra. Esto permite al diseñador detectar áreas con problemas.

Creación de diagramas de segmento de red

Luego, el diseñador crea diagramas para las disposiciones físicas y lógicas de las redes instaladas en cada uno de los distintos sitios.

Cada diagrama muestra:

- La ubicación del equipo de red y los armarios para el cableado
- La información de direccionamiento lógico
- La información de denominación

Al utilizar estos diagramas, el diseñador identifica qué partes del equipo o de la topología necesitan cambios. El diseñador evalúa los flujos de tráfico y las estructuras de direccionamiento.

Refiera a la **Figura** del curso en línea

La red instalada en la ubicación principal del estadio es más compleja que las redes de los sitios remotos particulares. El diseñador de red crea un diagrama lógico individual para mostrar todos los distintos componentes y topologías de la LAN. El diagrama muestra los flujos de tráfico entre los usuarios y los servidores.

Creación de un diagrama lógico de la LAN principal del estadio

El diseñador crea un diagrama lógico de la red que muestra las partes principales del equipo de sistema de redes y cómo se interconectan. Este diagrama incluye:

- Routers y switches
- ***Puntos de acceso inalámbrico***
- Equipo de telecomunicaciones esencial (CSU/DSU, módems, etc.)
- Firewalls y dispositivos de detección de intrusión (***IDS***, intrusion detection devices)
- Estaciones de administración
- Servidores y granjas de servidores

Todos los servidores y servicios se incluyen en el diagrama lógico. Esto se debe a que su ubicación puede afectar los patrones de tráfico, el uso del ancho de banda y la seguridad. El diseñador rotula cada una de las conexiones con el ancho de banda y el tipo de cable o dispositivo inalámbrico que se utiliza.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar el Asistente de Cisco Network y los comandos IOS de Cisco para crear un diagrama lógico de la red de CompañíaCinematográfica.

3.1.3 Desarrollo de un diagrama modular

Refiera a la **Figura** del curso en línea

La red del estadio ha crecido considerablemente desde su diseño inicial. El diseñador de CompañíadeRedes considera el diagrama lógico y organiza la red en un ***diagrama de bloques modulares***.

Un diagrama de bloques modulares es una versión simplificada de la red. El diagrama muestra las funciones principales en forma modular. Este diagrama permite al diseñador determinar la arquitectura subyacente sobre la que se crea la red.

El diseñador compara el diagrama de bloque con el diseño ideal de red representado por las ***Arquitecturas de redes empresariales*** de Cisco. El diseñador identifica las áreas que deben volver a diseñarse o actualizarse.

La arquitectura inicial de la red del estadio es una red plana grande. Sólo tiene dos capas físicas de switches. Algunos de los switches proporcionan conectividad de dispositivo final a la red y algunos interconectan otros switches. Ambas capas se crean utilizando switches de Capa 2 que no están segmentados por las VLAN.

Las ubicaciones de los servidores se encuentran en varios puntos dentro de la red.

La conectividad a Internet se proporciona a través de otro router. La conectividad se protege mediante un firewall y un IDS. Ambas ubicaciones remotas se conectan a la red del estadio a través de las VPN que terminan en el router de Internet.

Refiera a la actividad de “**Packet Tracer**” del curso en línea

Actividad de Packet Tracer

Crear un diagrama de bloques modulares de una red actual para poder identificar las debilidades en el diseño.

3.1.4 Fortalezas y debilidades de la red actual

Refiera a la **Figura** del curso en línea

Los diagramas creados por el diseñador de red permiten al personal de CompañíadeRedes analizar las fortalezas y debilidades de la red actual.

Fortalezas de la red actual del estadio

El diseñador revisa la documentación de red de video y voz actual para determinar las ubicaciones del equipo y los distintos grupos que utilizan los servicios.

Se instaló recientemente el nuevo cableado Categoría 5e en todo el complejo del estadio. Además, la nueva fibra monomodo conecta los armarios de cableado con el cuarto de telecomunicaciones principal. El rendimiento disponible proveniente del cableado existente disminuye la necesidad de realizar cambios en la infraestructura de la red del estadio. Sólo se agregará cableado si es necesario instalar los nuevos puntos de acceso.

Un área junto al armario para el cableado es ideal para la instalación del nuevo ***centro de datos*** que aloje la granja de servidores.

Refiera a la **Figura** del curso en línea

Luego de revisar los diagramas e inventarios del equipo existente, el diseñador de red menciona las fortalezas y debilidades de la red actual del estadio:

Fortalezas:

- Cableado nuevo y armarios para el cableado adecuados
- Espacio adecuado para un nuevo centro de datos

- Los servidores y las PC son modelos actuales y no necesitarán ser reemplazados
- Algunos routers y switches de la red existente pueden utilizarse en el nuevo diseño

Debilidades:

- Diseño de red plana
- No hay capa de distribución
- No hay capa núcleo verdadera
- Servidores mal ubicados
- Varias redes que pueden ser difíciles de mantener
- Estructura de direccionamiento IP inadecuada
- No hay ancho de banda dedicado para la conectividad WAN
- Servicio inalámbrico mal implementado
- Implementaciones de seguridad limitadas

Superación de las debilidades como preparación para la actualización de la red

El diseñador se enfoca en encontrar formas de superar las debilidades de la red actual. El diseñador propone actualizar el diseño de red realizando las mejoras necesarias.

También se evalúa el equipo que no se reemplazará durante la actualización. Es importante saber que el hardware funciona correctamente y que el software está actualizado para asegurar una integración fácil de las nuevas funciones de la red.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Investigue la red actual y haga una lista de fortalezas y debilidades.

3.2 Actualización del IOS de Cisco existente

3.2.1 Navegación y funciones de CCO de Cisco

Refiera a la **Figura** del curso en línea

El sitio Web Cisco.com brinda herramientas y recursos en línea para ayudar al personal de CompañíadeRedes a obtener información sobre el equipo de red del estadio. El sitio Web puede ayudar a resolver problemas técnicos comunes. Las herramientas y recursos incluyen lo siguiente:

- ***Documentación:*** verificación y configuración de software y hardware, además de resolución de problemas en tecnologías y productos Cisco
- ***Herramientas:*** solicitudes de servicio, evaluación, instalación y resolución de problemas
- ***Descargas:*** software, publicaciones de archivos específicos y aplicaciones de soporte técnico
- ***Comunidades y capacitación:*** información en el foro Networking Professionals Connection, asistencia a seminarios sobre soporte técnico y otras oportunidades de capacitación
- ***Noticias:*** temas actuales publicados en el Boletín de soporte técnico de Cisco

Para acceder a muchas de las funciones disponibles en Cisco.com, es necesario crear una cuenta de usuario registrado en Cisco.com. El nivel de acceso depende del tipo de cuenta de usuario y de si el usuario posee actualmente un contrato de mantenimiento SMARTnet.

3.2.2 Investigación del software IOS de Cisco instalado

Refiera a la **Figura** del curso en línea

Antes de utilizar las herramientas de Cisco.com, el personal de CompañíadeRedes necesita la siguiente información de la lista de inventario del equipo:

- Modelo y tipo de dispositivo
- Memoria instalada
- Interfaces y ranuras
- Módulos opcionales instalados
- Versión del software IOS actual y nombre de archivo

El personal de CompañíadeRedes utiliza esta información para determinar qué versión del software IOS de Cisco es adecuada y qué opciones de hardware pueden instalarse.

Uso del comando `show version`

Los técnicos utilizan el comando **`show version`** en cada dispositivo para verificar que la lista de inventario sea correcta. El comando también les permitirá obtener la información faltante.

Luego, el diseñador de red envía al personal una lista de las nuevas funciones. El diseñador considera que estas funciones serán necesarias para admitir las capacidades ampliadas de la red del estadio. La evaluación de la lista de nuevas funciones permite al personal seleccionar la versión del software IOS adecuada para la nueva red.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar el comando **`show version`** para completar una hoja de inventario para un switch y un router de Cisco.

Refiera a la **Figura** del curso en línea

El personal de CompañíadeRedes y el administrador de TI del estadio analizan cómo actualizar el equipo de red actual con una interrupción mínima de las operaciones cotidianas. Coinciden en que los routers y switches de la red pueden actualizarse durante el mantenimiento programado el domingo de 2:00 a.m. a 8:00 a.m. Sin embargo, debido a la gran cantidad de dispositivos instalados, la actualización puede necesitar más que la mañana del domingo para terminar.

En la red del estadio, se incluirán tres tipos de dispositivos de red en el nuevo diseño:

- 16 switches Cisco 2960
- 1 router Cisco 1841
- 3 routers que no son de Cisco

Una vez que el personal de CompañíadeRedes determina qué componentes de hardware y versiones del software IOS de Cisco necesitan instalarse, éste podrá calcular el tiempo necesario para actualizar el equipo de Cisco. Los routers que no son de Cisco se actualizarán posteriormente.

Normas de denominación IOS

Los archivos de IOS deben estar actualizados para prevenir riesgos de seguridad e implementar correcciones de errores. Algunos de los dispositivos instalados en la red del estadio incluyen versiones de IOS obsoletas.

Las ***normas de denominación IOS*** proporcionan el número de versión y el conjunto de funciones del IOS.

Refiera a la **Figura** del curso en línea

Cuando se actualiza el software IOS de Cisco en un switch o router, el dispositivo necesita reiniciarse. Este proceso interrumpe el funcionamiento del dispositivo durante un período breve. Al igual que con cualquier actualización, pueden surgir problemas imprevistos luego de cargar el

nuevo hardware o IOS. Las actualizaciones deben planificarse detalladamente. Esta medida asegurará que la red no se interrumpa durante el horario de funcionamiento normal.

Prueba del proceso de actualización

Para evitar la mayor cantidad posible de problemas, CompañíadeRedes obtiene un switch 2960 y un router 1841. Estos dispositivos se utilizan para probar el proceso de actualización antes de intentar actualizar el equipo del estadio. La prueba se considera una buena práctica ya que pueden haber diferencias significativas entre las versiones de IOS o los componentes de hardware.

La utilización del equipo de prueba permite al personal de CompañíadeRedes verificar que el sistema actualizado funcionará según lo previsto. También podrá calcular mejor la cantidad de tiempo que tardará la ejecución de cada actualización.

3.2.3 Elección de una imagen adecuada de IOS de Cisco

Refiera a la **Figura** del curso en línea

El personal de CompañíadeRedes necesita determinar si los dispositivos actuales pueden admitir una versión de IOS de Cisco con las nuevas funciones de red necesarias. Éste es un paso importante en el proceso de actualización.

Utilización del navegador de funciones

El sitio Web Cisco.com brinda herramientas para ayudar al personal de CompañíadeRedes a elegir la versión correcta del IOS. El ***Navegador de funciones*** es una herramienta Web que permite determinar cuáles son las funciones que una imagen de software IOS específica admite. El Navegador de funciones también puede utilizarse para buscar qué imágenes de software IOS admiten una función específica.

El Navegador de funciones permite realizar búsquedas por función o versión. En la sección de versiones, el personal compara una versión con otra. Los usuarios registrados en Cisco.com pueden acceder al Navegador de funciones en http://www.cisco.com/go/fn.

El software IOS se empaqueta en conjuntos de funciones que admiten plataformas de router y switch específicas. El personal utiliza el Navegador de funciones de Cisco para determinar qué versiones de IOS son adecuadas para el equipo instalado. También utiliza la lista de inventario y la lista de funciones necesarias que proporcionó el diseñador de red.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar el Navegador de funciones para seleccionar el software IOS de Cisco adecuado para la red de CompañíaCinematográfica y verificar que el dispositivo tenga suficiente ***DRAM*** y ***memoria flash*** para admitirlo.

Refiera a la **Figura** del curso en línea

El personal de CompañíadeRedes identifica una versión adecuada de la imagen del software IOS de Cisco. Después de ello, el personal debe verificar que cada dispositivo tenga suficiente ***memoria flash*** y ***RAM*** para admitir los nuevos archivos de IOS. De lo contrario, las actualizaciones de la memoria deben realizarse antes de instalar el nuevo IOS.

La compañía del estadio posee un acuerdo de mantenimiento que permite a los miembros del personal descargar las nuevas versiones de IOS para el equipo Cisco. El personal de CompañíadeRedes solicita a la administración del estadio que asegure el cumplimiento de los acuerdos de licencia de Cisco. Se debe verificar que cada dispositivo Cisco se incluya en el acuerdo de mantenimiento.

El personal de CompañíadeRedes descarga las nuevas versiones de IOS desde Cisco.com. Éstas pueden almacenarse luego en un servidor de Protocolo de transferencia de archivos trivial (***TFTP***, Trivial File Transfer Protocol). Al almacenar los archivos en un servidor TFTP, el personal puede cargar el software fácilmente en los routers y switches para realizar la actualización.

El comando `copy` se utiliza para transferir archivos de un servidor TFTP a un router o switch.

3.2.4 Descarga e instalación del software IOS de Cisco

Refiera a la **Figura** del curso en línea

Los switches y routers del estadio no tienen una versión actual de IOS de Cisco. Las actualizaciones necesarias deben realizarse en forma manual por medio de los siguientes pasos:

Paso 1: Seleccione una imagen del software IOS

El primer paso en el procedimiento de actualización es seleccionar la versión de la imagen del software IOS y el conjunto de funciones adecuados. Se deben considerar los siguientes factores al seleccionar una versión de IOS:

- **Requisitos de memoria**: compruebe que el router tenga suficiente memoria flash o espacio en disco para almacenar el IOS. El router también necesita tener suficiente memoria (***DRAM***) para ejecutar el IOS. Si el router no tiene suficiente memoria, puede tener problemas cuando se reinicie con el nuevo IOS.
- **Soporte de módulo e interfaz**: compruebe que el nuevo IOS admita todas las interfaces y módulos nuevos y actuales que se instalarán en el router.
- **Soporte de funciones de software**: compare las funciones del nuevo IOS con las que se utilizaban en el IOS anterior. Se deben incluir las nuevas funciones necesarias para la actualización de la red.

El personal de CompañíadeRedes utiliza el Navegador de funciones para encontrar las versiones de IOS adecuadas para el equipo instalado. El personal descarga y copia los archivos de IOS en el directorio de descarga del servidor TFTP. También lee las ***notas de la versión*** para comprobar que no hayan cambios imprevistos o problemas conocidos con la versión.

Refiera a la **Figura** del curso en línea

Paso 2: Identifique el sistema de archivos de dispositivos para copiar la imagen

El personal de CompañíadeRedes utiliza el resultado del comando **`show file systems`** para ubicar las imágenes o los archivos de IOS de Cisco. Se puede utilizar este comando o el comando **`dir`** *`[sistema_de_archivos]`* para encontrar el espacio libre disponible para almacenar las nuevas imágenes de IOS. Si los dispositivos no tienen suficiente memoria flash, se deben realizar actualizaciones de la memoria antes de instalar el nuevo IOS.

Paso 3: Verifique que el servidor TFTP tenga conectividad IP al dispositivo

El servidor TFTP debe tener una conexión de red al dispositivo. Debe ser capaz de hacer ping a la dirección IP del dispositivo destinado a una actualización de software TFTP. Para lograr esta conexión, la interfaz del dispositivo y el servidor TFTP deben tener configurados una dirección IP en el mismo rango o un gateway predeterminado.

Refiera a la **Figura** del curso en línea

Paso 4: Realice una copia de seguridad de las configuraciones actuales a modo de preparación para la actualización

Se debe realizar una copia de seguridad de los archivos de configuración y del IOS actual del router antes de actualizar IOS de Cisco. La configuración en ejecución debe copiarse en la configuración de inicio. Se debe realizar una copia de seguridad de la configuración de inicio y de la imagen del IOS actual en un servidor TFTP. Algunas de las versiones de IOS agregan configuraciones predeterminadas. Estos nuevos elementos de configuración pueden entrar en conflicto con la configuración actual.

Paso 5: Copie la imagen de IOS en el dispositivo

Cuando el personal de CompañíadeRedes haga ping entre el servidor TFTP y el dispositivo, podrá copiar la imagen del software IOS en la memoria flash. Antes de copiar la imagen, el personal comprueba que el software del servidor TFTP se esté ejecutando. Luego confirma que la imagen de IOS se encuentre en el directorio del servidor TFTP correspondiente.

Para actualizar el IOS desde un servidor TFTP, el personal utiliza el comando **`copy tftp flash`**.

El proceso de copiado demora varios minutos. El comando **`dir flash`** se utiliza para verificar que el archivo haya sido transferido con éxito.

Para completar la actualización, el personal de CompañíadeRedes reinicia el dispositivo y observa el proceso de arranque del mismo.

El personal realiza la actualización en los dispositivos de red de prueba. Luego de completar la actualización, compara las configuraciones resultantes con las configuraciones guardadas. El personal comprueba que las diferencias entre las configuraciones no afecten el funcionamiento de la red del estadio.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Packet Tracer

Descargue el IOS de Cisco correcto y transfiera el archivo al switch o router Cisco utilizando un servidor TFTP.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Preparar un router para recibir un nuevo IOS de Cisco y transferir el IOS al router desde un servidor TFTP.

3.2.5 Proceso de inicio del router

Refiera a la **Figura** del curso en línea

El ***proceso de arranque*** está conformado por tres etapas:

1. Ejecución de la POST y carga del programa bootstrap

La autocomprobación de encendido (***POST***, Power-On Self Test) es un proceso que ocurre en casi todas las computadoras durante el arranque. La POST se utiliza para probar el hardware del router.

Luego de la POST, se carga el programa bootstrap. El programa bootstrap ubica el IOS de Cisco y lo carga en la RAM.

2. Ubicación y carga del software IOS

La ubicación del archivo del IOS se especifica mediante el valor del parámetro de registro de configuración. Los bits de este parámetro pueden indicar al dispositivo que cargue el archivo del IOS desde las siguientes ubicaciones:

- La memoria flash
- Un servidor TFTP
- Otra ubicación indicada en el archivo de configuración de inicio

Para cargar el IOS normalmente desde la memoria flash, el parámetro del registro de configuración debe establecerse como 0x2102.

3. Ubicación y ejecución del archivo de configuración de inicio o ingreso al modo Setup

Luego de cargar el IOS, el programa bootstrap busca el archivo de configuración de inicio (startup-config) en la ***NVRAM***. El archivo contiene los parámetros y comandos de configuración previamente guardados, entre ellos:

- Direcciones de interfaz
- Información de enrutamiento

- Contraseñas
- Otros parámetros de configuración

Si no se encuentra el archivo de configuración, el router indica al usuario que ingrese al modo Setup para comenzar el proceso de configuración.

Si se encuentra un archivo de configuración de inicio, aparecerá una petición de entrada con el nombre de host. El router ha cargado exitosamente el IOS y el archivo de configuración. El personal de CompañíadeRedes puede comenzar a utilizar los comandos de IOS en el router.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Observar el proceso de inicio en un router 1841.

3.3 Actualización del hardware existente

3.3.1 Investigación de las funciones de hardware instaladas

Refiera a la **Figura** del curso en línea

Luego de actualizar las versiones de IOS de Cisco, el diseñador de red necesita saber cuáles son las actualizaciones del hardware que pueden realizarse en los dispositivos existentes para que cumplan con los nuevos requisitos. Las actualizaciones pueden ser necesarias para incluir módulos de alta densidad y alta velocidad, y otras opciones de hardware disponibles, como los kits de montaje en bastidor.

Cisco.com ofrece hojas de datos para todos los dispositivos instalados en la red del estadio. El personal de CompañíadeRedes utiliza estas hojas de datos para crear una lista de posibles opciones para cada dispositivo.

El personal utiliza la hoja de datos del router 1841 para saber qué módulos e interfaces se encuentran disponibles para ese modelo. Varios tipos diferentes de módulos coinciden con las dos ranuras para opciones en el 1841, entre ellos:

- Tarjetas de interfaz WAN (***WIC***, WAN interface cards)
- Tarjetas de interfaz WAN de alta velocidad (***HWIC***, High-speed WAN interface cards)
- Tarjeta de interfaz de WAN/de voz (***VWIC***, Voice/WAN interface cards)
- WIC inalámbricas que pueden funcionar como puntos de acceso
- HWIC Gigabit Ethernet para proporcionar conectividad de fibra

El diseñador utiliza esta lista para determinar qué opciones se necesitan para cumplir con los requisitos de la nueva red.

3.3.2 Investigación de las opciones de hardware adecuadas

Refiera a la **Figura** del curso en línea

Los dispositivos de hardware incluyen diferentes capacidades. Es importante entender qué tecnologías y medios admitiría un módulo en un router determinado. El diseñador de red considera las tecnologías que probablemente sean aplicables en el nuevo diseño para la red del estadio.

Para admitir el tráfico de datos, video y voz en la nueva red, el diseñador confecciona la siguiente lista de tecnologías y medios:

- Gigabit Ethernet que utiliza fibra en las capas de distribución y núcleo
- Conectividad de 100 Mbps con cable de cobre en la capa de acceso

- Gigabit Ethernet con cobre o fibra en el centro de datos
- Conexiones seriales de alta velocidad a los dos sitios WAN
- Línea de suscriptor digital de alta velocidad (***DSL***) para conectarse a Internet

El diseñador compara esta lista con la lista de opciones disponibles en la documentación para el router 1841 en Cisco.com. El 1841 existente puede admitir los módulos necesarios para conectarse al sitio WAN y a Internet.

Actividad en pantalla completa

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en el laboratorio

Investigar las opciones de hardware disponibles en el router de servicio integrado 1841.

3.3.3 Instalación de una nueva opción de hardware

Refiera a la **actividad de laboratorio** del curso en línea

Instalación de tarjetas de interfaz opcionales en un router 1841

El personal de CompañíadeRedes visita Cisco.com para buscar las instrucciones para instalar las tarjetas de interfaz opcionales. El procedimiento para instalar estas tarjetas es el siguiente:

Paso 1: Apague el router

Refiera a la **Figura** del curso en línea

Las ranuras opcionales del router 1841 no admiten tarjetas de interfaz opcionales ***intercambiables en caliente***, que pueden cambiarse mientras el dispositivo está encendido.

Paso 2: Retire la placa frontal de la ranura

Utilice un destornillador Phillips No. 1 o un destornillador pequeño de hoja plana para destornillar los tornillos imperdibles. Luego, reitre la ***placa frontal*** de relleno de la ranura del chasis.

Paso 3: Instale el módulo opcional

- Para minimizar el riesgo de sufrir una descarga estática y un daño al equipo durante el proceso de instalación, utilice una correa para muñeca antiestática conectada a tierra en forma adecuada al trabajar con equipo electrónico.
- Sostenga la tarjeta por los extremos para reducir el riesgo de daños por descargas estáticas.
- Alinee la tarjeta con las guías de las paredes del chasis o el divisor de ranura y deslícela suavemente hacia la ranura.
- Empuje la tarjeta hasta asegurar el conector del extremo. La placa no debe tocar el panel posterior del chasis.
- Asegure los tornillos imperdibles en la placa.

Paso 4: Encienda el router y verifique la nueva configuración

- Conecte una PC al puerto de la consola del router y observe el proceso de inicialización.
- Verifique si el router reconoce la nueva tarjeta de interfaz opcional.
- Observe la designación de interfaz que se asigna al nuevo dispositivo en la hoja de inventario y en el diagrama de la topología existente.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Agregar una tarjeta de interfaz opcional a un router 1841 y observar el inicio del router y las nuevas designaciones de interfaz.

3.4 Realización de un relevamiento del sitio inalámbrico

3.4.1 Visita al sitio del cliente

Refiera a la **Figura** del curso en línea

El siguiente paso en la descripción de la red actual es evaluar la implementación de la LAN (WLAN) inalámbrica en el estadio. Debido a diferencias en las configuraciones, la ubicación del punto de acceso (AP) y el entorno físico, cada WLAN es una instalación única.

Antes de finalizar el diseño de red inalámbrica, el personal de CompañíadeRedes realiza un relevamiento del sitio para determinar el mejor uso y ubicación de los componentes del sistema de red inalámbrica. El relevamiento proporciona la información necesaria para ayudar al diseñador de red a determinar el tipo, la ubicación y las áreas de cobertura de los puntos de acceso de la WLAN.

Para los relevamientos del sitio inalámbrico es necesario que el personal de CompañíadeRedes ingrese a espacios públicos, oficinas y otras ubicaciones donde se lleven a cabo operaciones comerciales.

El personal de CompañíadeRedes representa a la empresa siempre que se encuentra en el sitio del estadio. Al visitar un sitio del cliente, es importante comportarse de manera profesional y vestirse adecuadamente. El comportamiento y profesionalismo del personal refleja de manera positiva la capacidad de CompañíadeRedes de instalar la actualización.

Refiera a la **Figura** del curso en línea

Al prepararse para un relevamiento del sitio inalámbrico, el personal de CompañíadeRedes debe cumplir con las pautas de CompañíadeRedes.

Se prepararon las siguientes pautas para el relevamiento de sitio del estadio deportivo:

Preparación

- Programe el relevamiento del sitio con el cliente.
- Use vestimenta adecuada para la tarea.
- Porte o lleve credenciales de la empresa.
- Disponga del equipo adecuado (elabore una lista de verificación estándar para garantizar que esté incluido todo el material necesario).
- Notifique al personal del estadio cuándo llegará el personal y cuánto tardará el relevamiento del sitio.

Relevamiento del sitio

- Registre su entrada con el personal correspondiente al ingresar al estadio.
- Trabaje rápido y de manera profesional para inspirar confianza al cliente.
- Responda a las preguntas con cortesía y con el mayor detalle posible.
- Anote todas las preguntas que otros miembros del personal deberán responder.
- Informe al cliente sobre los procedimientos del relevamiento.
- Antes de retirarse de las instalaciones, informe al personal del cliente que el relevamiento se realizó de manera exitosa.

Seguridad

Muchas empresas cuentan con sus propios guardias de seguridad uniformados que necesitan estar informados sobre cualquier visita. Las empresas generalmente solicitan a un visitante que registre su entrada en la oficina principal antes de acceder a otras áreas. En áreas de alta seguridad,

es sumamente importante obtener permiso de seguridad y ser escoltado si es necesario. Entre las áreas de alta seguridad, se incluyen instalaciones militares, gubernamentales y de aviación.

Pautas de seguridad

- Cumpla con las pautas de seguridad recomendadas para garantizar una operación adecuada y un uso seguro de los dispositivos inalámbricos.
- Obtenga la autorización del cliente antes de tocar o conectar dispositivos a cualquier equipo existente del sistema de red.

Refiera a la **Figura** del curso en línea

Cuando CompañíadeRedes programa un relevamiento del sitio inalámbrico, el cliente puede establecer los requisitos de visita al sitio que el personal deberá cumplir. Es posible que algunas empresas no hayan establecido requisitos de visita al sitio si los proveedores no visitan sus instalaciones con frecuencia. En tal caso, el técnico de CompañíadeRedes debe realizar preguntas específicas para poder establecer los requisitos de visita al sitio al concertar la cita.

Algunos requisitos de visita al sitio pueden incluir:

- Limitaciones de acceso
- Vestimenta
- Equipo de seguridad
- Credenciales de identificación
- Horario de trabajo
- Seguridad
- Artículos prohibidos

Los requisitos del cliente pueden variar según el sitio. El personal de CompañíadeRedes debe cumplir con los requisitos del cliente cuando se prepara para visitar el sitio.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Programar una cita para realizar un relevamiento del sitio inalámbrico.

3.4.2 Consideraciones físicas de la red

Refiera a la **Figura** del curso en línea

La red del estadio actualmente proporciona acceso inalámbrico limitado a través de dos puntos de acceso (AP, access points). Un AP se encuentra en el área de la oficina del equipo. Este AP en realidad es un router inalámbrico pequeño que compró la administración del equipo. El otro AP, un AP Cisco Aironet económico y más antiguo, está ubicado en la cabina de prensa del estadio. Este AP proporciona acceso inalámbrico a los periodistas.

En el diseño de red propuesto, la red del estadio necesita más zonas activas inalámbricas en las suites de lujo y en el restaurante del estadio. En ambas ubicaciones, la administración del estadio planea ofrecer acceso inalámbrico no protegido a Internet.

El diseñador de red ha identificado una lista de posibles fuentes de interferencia y algunos problemas en la infraestructura física del estadio que pueden afectar las áreas de cobertura de radiofrecuencia. Durante el relevamiento del sitio, el personal de CompañíadeRedes puede verificar estas áreas para determinar el impacto real en las señales inalámbricas.

Entre las áreas de interés del diseñador se incluyen:

- Hornos microondas ubicados en las áreas de concesión y palcos de lujo
- Teléfonos inalámbricos y auriculares utilizados por periodistas y reporteros

- Ejes de ascensor ubicados cerca de las áreas externas del restaurante y las suites de lujo
- Paredes y pilares gruesos de cemento entre las suites de lujo

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de página completa

3.4.3 Planificación y relevamiento del sitio inalámbrico

Refiera a la **Figura** del curso en línea

La realización de un relevamiento del sitio consta de los siguientes pasos:

Paso 1: Defina los requisitos del cliente

El estadio quizá desee publicar la disponibilidad de zonas activas inalámbricas. El personal de CompañíadeRedes necesita determinar las expectativas del nivel de servicio. También es necesario determinar si el estadio desea admitir tecnologías inalámbricas avanzadas, como teléfonos IP inalámbricos.

Paso 2: Identifique las áreas de cobertura

El personal de CompañíadeRedes calcula la cantidad de usuarios potenciales en cada área de cobertura. Más importante aún, el personal determina el horario pico previsto durante los eventos principales.

Paso 3: Determine las ubicaciones preliminares de los puntos de acceso

El personal revisa los planos del estadio y sugiere posibles ubicaciones de los puntos de acceso. Luego, se determina de qué manera se puede proporcionar cobertura, qué áreas necesitan suministro eléctrico y cómo se conectarán los puntos de acceso a la red cableada.

Paso 4: Mida la potencia de la señal

El personal instala temporalmente un punto de acceso en una ubicación propuesta. Luego mide la potencia de radiofrecuencia recibida y las posibles causas de interferencia.

Refiera a la **Figura** del curso en línea

El personal de CompañíadeRedes instala un punto de acceso temporario en el centro del restaurante, lejos de la cocina. No es necesario que el punto de acceso esté conectado a la red del estadio ya que sólo se prueba la cobertura inalámbrica.

Para realizar la prueba, el personal utiliza una computadora portátil equipada con una herramienta de relevamiento del sitio en una NIC inalámbrica.

El personal de CompañíadeRedes realiza los siguientes pasos:

Paso 1: Mide la potencia de la señal y la velocidad de un enlace a medida que se aleja del punto de acceso.

Paso 2: Registra las lecturas y mide las distancias con respecto al punto de acceso cuando cambia la calidad o la velocidad del enlace.

Paso 3: En un plano de la planta, marca las áreas donde las señales son aceptables.

El diseñador de red utiliza el plano de la planta marcado para determinar la ubicación de los puntos de acceso y los conectores cableados que los enlazan a la red. Luego de completar el tercer paso, el diseñador debe asegurarse de cumplir con todos los códigos de electricidad e incendio a nivel local, estatal y nacional.

Actividad de Packet Tracer

Refiera a la actividad de “**Packet Tracer**” del curso en línea

Colocar los puntos de acceso en diferentes ubicaciones utilizando un diagrama que incluya un plano de la planta de CompañíaCinematográfica.

Refiera a la **actividad de laboratorio** del curso en línea

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en el laboratorio

Realizar un relevamiento del sitio inalámbrico utilizando un punto de acceso y una NIC inalámbrica.

Pantalla completa

Jugar el juego Cisco Wireless Explorer.

3.5 Documentación de los requisitos de diseño de red

3.5.1 Creación de un documento de requisitos de diseño de red

Refiera a la **Figura** del curso en línea

El personal de CompañíadeRedes ahora ha completado las fases de preparación y planificación del ciclo de vida de actualización de la red. Está listo para crear un documento de requisitos de diseño y comenzar a diseñar la nueva red del estadio.

Un documento de requisitos de diseño es un resumen de todos los requisitos técnicos y empresariales principales para el diseño de la nueva red.

Gran parte de la información necesaria para completar el documento de requisitos de diseño se puede encontrar en la Solicitud de propuesta (RFP, Request for Proposal). El documento de requisitos de diseño contiene las especificaciones para la actualización de red propuesta.

Las primeras dos secciones del documento de requisitos de diseño son Objetivo general del proyecto y Alcance del proyecto.

Objetivo general del proyecto

Esta sección establece los objetivos generales de la actualización. También especifica de qué manera esta actualización ayudará a la empresa que administra el estadio a ser más exitosa.

Alcance del proyecto

Esta sección describe las áreas físicas, las aplicaciones y los grupos de usuarios afectados por la actualización de la red. También puede mencionar los componentes de la red que se encuentran fuera del alcance de su actualización, como las actualizaciones de una aplicación o un servidor.

Refiera a la **Figura** del curso en línea

Otras dos secciones importantes del documento de requisitos de diseño son Requisitos de la red y Estado actual de la red.

Requisitos de la red

Esta sección detalla todos los objetivos comerciales y requisitos técnicos, limitaciones, grupos de usuarios y aplicaciones que influyen en el diseño de la red del estadio propuesta.

Estado de la red

Esta sección detalla la red existente e incluye la siguiente información:

- Diagramas físicos y lógicos
- Listas de equipos
- Aplicaciones
- Fortalezas y debilidades

Refiera a la **Figura** del curso en línea

El diseñador de red debe conocer la red actual. De esta manera, el diseñador puede atender las debilidades y aprovechar las fortalezas con mayor eficiencia.

CompañíadeRedes revisa el documento de requisitos de diseño junto con la administración del estadio. Esto se realiza para garantizar que no haya confusiones antes de continuar con el proyecto de diseño.

3.5.2 Objetivo general del proyecto

Refiera a la **actividad de laboratorio** del curso en línea

Al redactar un objetivo general del proyecto, es importante considerar la finalidad principal del proyecto de diseño de la red. El objetivo general debe estar relacionado con los objetivos de la empresa, que están diseñados para que la empresa sea más exitosa.

En esta sección del documento, el diseñador de CompañíadeRedes describe el objetivo general del proyecto para la actualización de la red del estadio. El diseñador considera toda la información obtenida a partir de entrevistas con el presidente de EstadioCompañía y diálogos con otros miembros del personal del estadio.

CompañíadeRedes obtiene el consentimiento de la administración del estadio con respecto al objetivo general del proyecto.

Actividad en el laboratorio

Formular una declaración del objetivo general del proyecto para CompañíaCinematográfica.

3.5.3 Alcance del proyecto

Refiera a la **Figura** del curso en línea

La segunda sección del documento de requisitos de diseño describe el alcance del proyecto. Detalla qué porcentaje de la red se ve afectado o cambia como resultado del proyecto.

También define las partes de la red existente que no se incluyen dentro de las áreas que abarca el proyecto. Estas áreas fuera de alcance se definen para no generar confusión entre CompañíadeRedes y la administración de EstadioCompañía.

El diseñador de CompañíadeRedes observa la topología de la red actual y los servicios que ofrece. El objetivo general indica que tanto las redes WAN como las LAN deberán actualizarse. El alcance de este proyecto afecta a todos los usuarios que se encuentren en la instalación principal del estadio y en las dos ubicaciones remotas.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad

Determinar el alcance de distintas alternativas de actualización de la red.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear una declaración del alcance para CompañíaCinematográfica.

3.5.4 Objetivos empresariales y requisitos técnicos

Refiera a la **Figura** del curso en línea

Las primeras dos secciones del documento de requisitos de diseño generalmente son breves y no contienen demasiada información. Por el contrario, la sección Requisitos de la red es muy detallada. Esta sección permite guiar el diseño de red y la implementación de nuevas tecnologías.

La sección Requisitos de la red incluye los siguientes cuatro apartados:

- Objetivos empresariales
- Requisitos técnicos
- Usuarios
- Aplicaciones

Objetivos empresariales

El diseñador de CompañíadeRedes menciona los objetivos por orden de prioridad. Los objetivos más importantes se mencionan primero.

Refiera a la **Figura** del curso en línea

Requisitos técnicos

El diseñador de CompañíadeRedes evalúa cada uno de los objetivos comerciales. Luego determina los requisitos técnicos necesarios para cumplir con los objetivos. Estos requisitos se describen en la sección Requisitos técnicos según las características de escalabilidad, disponibilidad, seguridad y facilidad de administración.

- **Escalabilidad**: uno de los objetivos empresariales es agregar a la red nuevos servicios y usuarios, además de capacidad de video y voz. La red debe ser capaz de ampliarse fácilmente sin interrupciones o rediseños significativos de los servicios. El diseñador analiza y documenta los cálculos de crecimiento posible junto con la administración del estadio.
- **Disponibilidad**: al agregar voz, seguridad, video y venta de entradas en línea es necesario que la red se encuentre disponible para los usuarios en todo momento. Las nuevas aplicaciones deben ser accesibles para los sitios remotos y la ubicación principal del estadio. Las nuevas aplicaciones para el ingreso y la venta de entradas requieren de períodos de transacción muy breves. Para la incorporación de voz y video, es necesario que la red admita QoS.
- **Seguridad**: uno de los objetivos principales de todas las actualizaciones de una red es mejorar la seguridad. La red del estadio propuesta incluirá firewalls, filtrado y un sistema de detección de intrusión (IDS, intrusion detection system) para protegerla contra acceso de usuarios no autorizados. Los servicios se protegerán utilizando la granja de servidores del centro de datos.
- **Facilidad de administración**: la empresa que administra el estadio no desea aumentar la cantidad de personal de TI para mantener la nueva red. Por lo tanto, la red debe ser fácil de administrar y mantener. Una red es más fácil de administrar cuando se utilizan estándares de sistema de redes durante el diseño y la instalación. Para ayudar al mantenimiento de la red, es necesaria una aplicación de administración que brinde informes y alertas al departamento de TI. También se debe capacitar al personal de TI del estadio para que puedan administrar y mantener la red propuesta.

Refiera a la **Figura** del curso en línea

Usuarios

En esta sección del documento de requisitos de diseño se mencionan los diferentes grupos de usuarios y sus requisitos de acceso. La empresa que administra el estadio desea que clientes, proveedores, personal del equipo y trabajadores remotos tengan acceso a la red. Establece disposiciones similares para el personal administrativo de la empresa que se encuentra en el lugar de trabajo. Cada uno de estos grupos puede tener requisitos específicos para los servicios de red. Es importante documentar estos requisitos para que sean considerados al diseñar la red.

Aplicaciones

Las características del tráfico de la red y los requisitos de distintas aplicaciones afectan el diseño de la red. Esta sección del documento describe los tipos de aplicaciones que debe admitir la red. También se mencionan los requisitos específicos del tráfico de la red.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad

Actividad en el laboratorio

Refiera al **Gráfico Interactivo** del curso en línea

Desarrollar la sección Requisitos de red para el documento de requisitos de diseño de CompañíaCinematográfica.

3.5.5 Caracterización de la red actual

Estado de la red actual

Refiera a la **Figura** del curso en línea

La sección final del documento de requisitos de diseño incluye la siguiente información:

- Todos los diagramas de red que CompañíadeRedes crea para ilustrar la red actual
- Los nombres y direcciones IP de los servidores y los componentes importantes del sistema de red
- Las fortalezas y debilidades de la red actual y cómo afectan los objetivos comerciales

El diseñador de red crea una tabla que menciona cada una de las debilidades detectadas, qué objetivo técnico o comercial se ve afectado y de qué manera se puede eliminar la debilidad en el diseño de red propuesto.

El personal de CompañíadeRedes revisa el documento de requisitos de diseño terminado. Luego se programa una reunión con los ejecutivos de la empresa que administra el estadio. El propósito de la reunión es obtener el consentimiento y la autorización para continuar con el diseño de la actualización.

Actividad

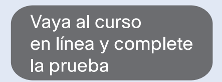
Refiera al **Gráfico Interactivo** del curso en línea

Actividad en el laboratorio

Refiera a la **actividad de laboratorio** del curso en línea

Analizar la red actual de CompañíaCinematográfica en relación con sus objetivos comerciales y requisitos técnicos.

Resumen del capítulo



Examen del capítulo

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 4

Identificación de los impactos de las aplicaciones en el diseño de la red

Introducción

Refiera a la **Figura** del curso en línea

4.1 Descripción de las aplicaciones de red

4.1.1 La importancia del rendimiento de las aplicaciones

Refiera a la **Figura** del curso en línea

La mayoría de las personas que utilizan servicios de red conocen muy poco sobre la red subyacente o el diseño de la red. Su experiencia como usuarios se basa en la forma en la que interactúan con las aplicaciones que se ejecutan en la red.

En el caso del estadio deportivo, las aplicaciones basadas en red proporcionan servicios esenciales para los aficionados, los equipos y la administración. Estos servicios, y la red en la que residen, se incluyen entre los elementos esenciales de la empresa para asegurar el cumplimiento de las demandas de los usuarios y el cliente.

La recopilación de información estadística de routers, servidores y otros dispositivos de red permite determinar si un sistema funciona según las especificaciones del fabricante. Sin embargo, las consideraciones técnicas por sí solas no determinan el éxito en el mercado.

El éxito depende de la opinión del cliente, los proveedores y los distribuidores sobre el rendimiento de la red.

Para los usuarios finales, el rendimiento de la aplicación se basa en lo siguiente:

- Disponibilidad: ¿la aplicación funciona cuando es necesario?
- Capacidad de respuesta: ¿la aplicación responde con la rapidez esperada?

Por ejemplo, en el estadio, las ganancias obtenidas por la venta de entradas, las concesiones y los recuerdos se ven afectadas cuando los procesos de transacción no se encuentran disponibles o tardan demasiado en completarse.

Refiera a la **Figura** del curso en línea

Los clientes del estadio evalúan la conveniencia de una aplicación según el tiempo que tarda en completar la transacción. También esperan que la aplicación se encuentre disponible cada vez que deseen usarla.

Entre las aplicaciones en donde se considera esencial un tiempo rápido de respuesta para el usuario se incluyen:

- Servicios de quiosco interactivo
- Máquinas de punto de venta de entradas
- Registros de concesión

Entre las aplicaciones que el personal del estadio considera esenciales se incluyen:

- Servicios de emergencia
- Transmisión y monitoreo de video y voz

Refiera a la **Figura** del curso en línea

La medida del rendimiento de la aplicación debe combinar la satisfacción del usuario con las métricas técnicas normales, como el rendimiento en la red o la cantidad de transacciones exitosas.

4.1.2 Características de las diferentes categorías de aplicaciones

En una red existente, la ***caracterización de la aplicación*** permite al diseñador de red incorporar objetivos empresariales y requisitos técnicos en el diseño de red.

El proceso de caracterización de la aplicación implica considerar los siguientes aspectos de las aplicaciones de red:

- Cómo funcionan las aplicaciones en la red
- Los requisitos técnicos de la aplicación
- Cómo interactúan entre sí las aplicaciones en la red

A partir de la información recopilada durante las primeras fases del proceso de diseño, el diseñador determina qué aplicaciones se consideran esenciales para la empresa. El diseñador estima de qué manera funcionarán estas aplicaciones con la red propuesta.

El proceso de caracterización proporciona información sobre el uso de ancho de banda en la red y los tiempos de respuesta de las aplicaciones específicas. Estos parámetros influyen en las decisiones de diseño, entre ellas:

- Selección del medio de transmisión
- Cálculos del ancho de banda requerido

El tráfico proveniente de distintos tipos de aplicaciones genera diversas demandas de red. El diseñador de red reconoce cuatro tipos principales de comunicación de aplicaciones:

- ***Cliente a cliente***
- ***Cliente a servidor distribuido***
- ***Cliente a granja de servidores***
- ***Cliente a extremo empresarial***

Refiera a la **Figura** del curso en línea

En una red existente, el primer paso en la caracterización de la aplicación es recolectar la mayor cantidad posible de información sobre la red. Esto incluye recolectar información de lo siguiente:

- Información de la organización
- Auditoría de la red
- Análisis de tráfico

Información de la organización

La información de la organización consiste en documentación existente sobre la red y la opinión oral del personal del estadio. Durante las primeras fases de diseño es fácil obtener información, pero no siempre es confiable. Por ejemplo, los cambios en las aplicaciones, como las actualizaciones o el software instalado por el usuario, pueden pasar inadvertidos o no documentarse.

Auditoría de red

Una auditoría de red recolecta información sobre los dispositivos de red, monitorea el tráfico y revela detalles sobre la configuración de la red existente.

Análisis de tráfico

El análisis de tráfico proporciona información sobre la manera en que las aplicaciones y los protocolos utilizan la red. Puede revelar deficiencias en la red. Por ejemplo, muchas aplicaciones de gran ancho de banda que utilizan el mismo medio pueden generar grandes cantidades de tráfico. Esto puede representar una posible debilidad en el diseño actual.

Herramientas incorporadas en el software IOS de Cisco

El reconocimiento de aplicaciones basado en la red (***NBAR***, Network-Based Application Recognition) es una utilidad de Cisco que realiza auditorías y análisis de tráfico. El NBAR es un motor de clasificación que reconoce una amplia variedad de aplicaciones. El NBAR reconoce protocolos basados en la Web y otros de difícil clasificación que utilizan asignaciones de puerto UDP y TCP dinámicas.

Otra herramienta es ***NetFlow*** de IOS de Cisco. NetFlow proporciona de manera eficiente un conjunto de servicios para las aplicaciones IP. Estos servicios incluyen:

- Contabilización del tráfico de la red
- Facturación de la red según el uso
- Planificación de la red
- Seguridad
- Capacidades de monitoreo de denegación de servicio
- Monitoreo de la red

NetFlow proporciona información valiosa sobre aplicaciones y usuarios de la red, horarios pico de uso y enrutamiento del tráfico.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar NetFlow para caracterizar las aplicaciones de red que se utilizan en una red.

4.1.3 Cómo afecta el flujo de tráfico al diseño de red

Refiera a la **Figura** del curso en línea

Como parte de la caracterización de la aplicación, es necesario determinar el flujo de tráfico externo e interno en la red.

Tráfico interno

El ***tráfico interno*** lo generan los hosts locales y se destina a otros hosts dentro de la red del campus. Al diagramar los flujos de tráfico interno se pueden mostrar áreas donde se necesitan conexiones de gran ancho de banda además de identificar posibles cuellos de botella donde el tráfico puede congestionarse. Estos diagramas ayudan al diseñador a seleccionar la infraestructura y el equipo adecuados para admitir los volúmenes de tráfico.

Tráfico externo

El ***tráfico externo*** se define como tráfico que inician los usuarios fuera de la red local al igual que el tráfico que se envía a destinos ubicados en redes remotas. Algunos tipos de tráfico externo, como los servicios de emergencia o financieros, requieren de redundancia y presentan inquietudes de seguridad adicionales. El diseñador diagrama este tráfico a fin de determinar la ubicación de los firewalls y las redes DMZ, al igual que los requisitos de conectividad a Internet.

El diseñador analiza los flujos de tráfico externo e interno utilizando NBAR y Netflow. Para garantizar la utilización eficiente del ancho de banda de la red, NBAR puede utilizarse para identificar y clasificar tipos de tráfico a fin de aplicar mecanismos de QoS.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de pantalla completa

4.1.4 Cómo afectan las características de las aplicaciones al diseño de red

Refiera a la **Figura** del curso en línea

Los tipos de hardware instalados en una red afectan el rendimiento de una aplicación. Una red compleja, como la red del estadio deportivo, contiene muchos tipos diferentes de hardware. Cada uno de estos tipos de dispositivos puede retardar la velocidad de respuesta de la aplicación a las solicitudes de los usuarios. El retardo afecta la satisfacción del cliente con respecto al rendimiento de la aplicación. Por ejemplo, las aplicaciones utilizadas para voz y video pueden verse afectadas por retardos del hardware, lo cual puede degradar el rendimiento. Los retardos del hardware pueden producirse por lo siguiente:

- El tiempo de procesamiento que tarda un router en enviar el tráfico
- Los switches más antiguos que no pueden manejar las cargas de tráfico que las aplicaciones modernas generan

Una forma de garantizar un alto rendimiento es utilizar un enfoque de arriba hacia abajo. El enfoque de arriba hacia abajo adapta el diseño de la infraestructura física a las necesidades de las aplicaciones de red. Los dispositivos de red se eligen sólo luego de realizar un análisis detallado de los requisitos técnicos.

Las aplicaciones de red en una red moderna producen un rango de paquetes. Estos paquetes son de distintos tamaños y poseen diferentes conjuntos de protocolos, tolerancias al retardo y otras características. Cuando los requisitos de servicio de estas diferentes aplicaciones entran en conflicto entre sí, se pueden generar problemas en el rendimiento. Al agregar una nueva aplicación, el diseñador de red necesita considerar el impacto sobre el rendimiento de las aplicaciones existentes. El diseñador debe considerar el rendimiento previsto de la aplicación con condiciones de red y configuraciones cambiantes.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de pantalla completa

4.2 Descripción de las aplicaciones de red comunes

4.2.1 Procesamiento de transacciones

Refiera a la **Figura** del curso en línea

Actualmente, las aplicaciones de red representan el eje central de la actividad empresarial. Para cumplir con los objetivos empresariales del cliente, el diseñador de red debe asegurar el rendimiento de la aplicación. Sin embargo, cada aplicación o tipo de tráfico y cada combinación de aplicaciones en particular posee requisitos diferentes que pueden generar problemas en el rendimiento.

Entre los tipos más comunes de aplicación se incluyen:

- Aplicaciones de procesamiento de transacciones
- Aplicaciones de streaming en tiempo real
- Aplicaciones de correo electrónico y transferencia de archivos

- Aplicaciones Web y HTTP
- Servicios de dominio de Microsoft

Aplicaciones de procesamiento de transacciones

El procesamiento de transacciones es un tipo de procesamiento en el que la computadora responde de inmediato a las solicitudes del usuario. Cada solicitud que el usuario genera es una transacción. Estas transacciones pueden requerir la ejecución de operaciones adicionales en respuesta a la solicitud original. Por este motivo, las transacciones de aplicación son una consideración particular en el diseño de red.

Como ejemplo de un proceso de transacción, considere qué sucede cuando un cliente compra entradas en línea para un evento en el estadio deportivo.

Esta única transacción genera las siguientes operaciones en la red:

- Tráfico Web desde el cliente hasta la red
- Transacciones de base de datos
- Transacción de pedido del cliente
- Transacción de procesamiento de pedidos
- Transacción de entrega/envío

Refiera a la **Figura** del curso en línea

No todo el tráfico que entra o sale de una red se considera un proceso de transacción. Una transacción válida debe cumplir con los siguientes criterios:

- Debe ser atómica.
- Debe ser consistente.
- Debe ser aislada.
- Debe ser duradera.

Transacción atómica

Una ***transacción atómica*** garantiza que se han realizado todas las tareas de una transacción, o bien, que ninguna de ellas se ha realizado. Si la transacción no se procesa por completo, entonces toda la transacción se considera nula.

Transacción consistente

Una transacción consistente asegura el rechazo de transacciones incompletas. Si se produce una transacción incompleta, el sistema vuelve al estado en el que se encontraba antes de comenzar la transacción.

Transacción aislada

Una transacción aislada está protegida de todas las demás transacciones en la red. La seguridad es una consideración fundamental al diseñar la red. Las opciones de seguridad incluyen la incorporación de listas de control de acceso (***ACL***, access control lists), ***encriptación*** y firewalls a la topología de la red.

Transacción duradera

Una transacción duradera garantiza que la transacción no pueda deshacerse una vez completada, incluso luego de una falla del sistema. Un diseño duradero para los procesos de transacción requiere de redundancia en varios niveles. Estos niveles incluyen las conexiones de la capa física, los servidores, los dispositivos de conmutación y los routers.

Refiera a la **Figura** del curso en línea

El diseñador de red evalúa las herramientas de seguridad y redundancia que admiten las aplicaciones de procesamiento de transacciones.

Redundancia

Al incorporar aplicaciones de transacción, es necesario que el diseñador considere el impacto de cada transacción en la red. Este proceso es esencial, ya que posiblemente se necesiten dispositivos o cableado adicional para proveer la redundancia o el rendimiento disponible que requieren estas transacciones. La incorporación de redundancia a una red ofrece las siguientes ventajas:

- Reducción o eliminación del tiempo de inactividad de la red
- Mayor disponibilidad de aplicaciones

Las redes con redundancia eliminan el problema de los puntos únicos de falla. Si una ruta o un dispositivo fallan, la ruta o el dispositivo redundante pueden completar el proceso o la transacción. Los servidores que manipulan procesos de transacción tienen una ruta alternativa para recibir o entregar tráfico. Esto ayuda a asegurar que la aplicación se encuentre disponible cuando el cliente lo solicite.

Los dispositivos de red también pueden configurarse para obtener redundancia. Los dos protocolos comunes son:

- Protocolo rápido de árbol de extensión (***RSTP***, Rapid Spanning Tree Protocol)
- Protocolo de enrutamiento en espera activa (***HSRP***, Hot Standby Routing Protocol)

El RSTP evita los bucles de conmutación de Capa 2 que pueden producirse con switches redundantes.

El HSRP puede proveer redundancia de Capa 3 en la red. Este protocolo proporciona una conmutación por error inmediata o específica del enlace y un mecanismo de recuperación.

Los dispositivos y enlaces redundantes pueden implementarse en el diseño propuesto de la red del estadio en las capas de distribución y núcleo.

Refiera a la **Figura** del curso en línea

Seguridad

La seguridad es siempre un factor fundamental. Afecta no sólo a los procesos de transacción, sino también a todas las aplicaciones y al tráfico dentro de una red interna y externa. La protección de la privacidad, la integridad de la información de transacciones y la base de datos de las transacciones deben ser el centro de las consideraciones de seguridad. El diseñador de red analiza las posibilidades de acceder a los datos de las transacciones de manera inadecuada o alterarlos.

Las VPN utilizan un proceso denominado tunneling. Tunneling se conoce generalmente como “redireccionamiento de puertos” (port forwarding). Es la transmisión de datos a través de una red pública, que está dirigida a una red privada. El tunneling se logra al encapsular los datos de la red privada y la información de protocolo dentro de las unidades de transmisión de la red pública.

Los sistemas de detección de intrusión (IDS, intrusion detection systems) se utilizan para monitorear el tráfico de la red en busca de actividades sospechosas. Si se detecta alguna actividad sospechosa, el IDS alerta al sistema o al administrador. Un IDS puede configurarse para que impida que la dirección IP de origen del usuario tenga acceso a la red.

Los firewalls filtran tráfico basándose en una serie de criterios. La complejidad de la configuración del firewall puede provocar retardos. Se debe considerar el posible impacto que pueden generar los retardos en el diseño de una red.

Las ACL pueden filtrar el tráfico potencialmente peligroso que intenta ingresar a la red e impedir que un tráfico determinado salga de la red. Estos controles de acceso pueden retardar el proceso

de transacción. Se debe considerar la naturaleza apremiante de algunas transacciones al configurar las ACL.

4.2.2 Voz y streaming en tiempo real

Refiera a la **Figura** del curso en línea

Aplicaciones en tiempo real

Al diseñar la red para incluir aplicaciones en tiempo real, el diseñador de red debe considerar de qué manera la infraestructura de la red afectará el rendimiento de las aplicaciones.

Estas consideraciones incluyen los elementos físicos de la infraestructura:

- Conexiones y dispositivos de hardware
- Topología de la red
- Redundancia física

Las consideraciones lógicas incluyen de qué manera la configuración de QoS y las soluciones de seguridad afectan el tráfico. Todos estos factores afectan la manera en que el diseñador implementará soluciones de red, como los servicios de ***telefonía IP***.

Las aplicaciones de streaming en tiempo real presentan requisitos exclusivos para el diseño de la red. La única aplicación en tiempo real que se utiliza actualmente en el estadio es la vigilancia con video. La telefonía IP se incluye en la actualización de la red propuesta. El tráfico desde estas aplicaciones debe enviarse con la menor latencia y fluctuación posible.

Al determinar los objetivos empresariales y requisitos técnicos para el cliente, se deben analizar todos los aspectos de la red para garantizar una admisión e implementación adecuadas de las aplicaciones en tiempo real.

Refiera a la **Figura** del curso en línea

Infraestructura

Para admitir las aplicaciones en tiempo real propuestas y existentes, la infraestructura debe incluir las características de cada tipo de tráfico.

El diseñador de red debe determinar si los switches y el cableado existentes pueden admitir el tráfico que se agregará a la red. El cableado que puede admitir transmisiones en gigabits debe ser capaz de transportar el tráfico generado sin necesitar ningún cambio en la infraestructura. Los switches más antiguos quizá no admitan Power over Ethernet (***PoE***). El cableado obsoleto quizá no admita los requisitos de ancho de banda. Los switches y el cableado necesitarán ser actualizados para admitir estas aplicaciones.

VoIP

Al introducir ***VoIP*** en una red que utiliza teléfonos tradicionales, es importante recordar que VoIP utiliza routers que sean compatibles con voz. Estos routers convierten la voz analógica de señales telefónicas tradicionales en paquetes IP.

Una vez convertida en paquetes IP, el router envía dichos paquetes entre las ubicaciones correspondientes. Los routers que admiten voz deben agregarse al diseño.

Telefonía IP

En la telefonía IP, el teléfono IP realiza la conversión de voz a IP por sí mismo. No se requieren routers que admitan voz en la red de la empresa. Los teléfonos IP pueden utilizar el ***Administrador de comunicaciones unificadas de Cisco*** como servidor para la señalización y el control de llamadas. Los requisitos de la red del estadio incluyen telefonía IP.

Refiera a la **Figura** del curso en línea

Protocolos de video en tiempo real

La red debe ser capaz de admitir aplicaciones que requieran entregas vulnerables a retardos a fin de transportar streaming media de manera eficaz. El Protocolo de transporte en tiempo real (***RTP***, Real-Time Transport Protocol) y el Protocolo de control de transporte en tiempo real (***RTCP***, Real-Time Transport Control Protocol) admiten este requisito.

RTP y RTCP habilitan el control y la escalabilidad de los recursos de red al permitir la incorporación de mecanismos de QoS. Estos mecanismos de QoS proporcionan herramientas valiosas para minimizar problemas de latencia en aplicaciones de streaming en tiempo real. Estas herramientas incluyen colas de prioridad, colas personalizadas, ***colas de latencia baja*** y colas equitativas ponderadas en función de clases.

Uno de los requisitos técnicos del estadio es permitir que la grabación de los eventos que se celebran en el estadio se visualice en tiempo real desde cualquier parte del mismo.

4.2.3 Correo electrónico y transferencia de archivos

Refiera a la **Figura** del curso en línea

Las transferencias de archivos colocan grandes volúmenes de tráfico en la red. Este tráfico puede tener un impacto mayor sobre el rendimiento que las conexiones interactivas de extremo a extremo. Si bien las transferencias de archivos necesitan un gran rendimiento, generalmente tienen pocos requisitos de tiempo de respuesta.

Algunas de las características del tráfico de transferencia de archivos incluyen:

- **Uso de ancho de banda impredecible**: este tipo de tráfico generalmente es iniciado por el usuario; por lo tanto, no puede predecirse de manera confiable.
- **Paquetes de gran tamaño**: FTP y otros tráficos de transferencia de archivos utilizan paquetes de gran tamaño para lograr una transferencia eficiente. Estos paquetes grandes pueden provocar retardos en otros tipos de tráfico cuando se congestiona la red.

Como parte de la caracterización inicial de la red, es importante identificar la cantidad de usuarios que utilizan transferencias de archivos en forma regular. FTP no es el único tipo de tráfico de transferencia de archivos que normalmente se presenta en una LAN. La copia de archivos desde las unidades de red compartidas y la descarga de archivos grandes utilizando HTTP tienen características similares a FTP.

Según esta información, el diseñador de red puede anticipar los requisitos de rendimiento. Si estos requisitos superan la capacidad de la red, es necesario implementar medidas de QoS para garantizar el rendimiento de las aplicaciones vulnerables a retardos.

Refiera a la **Figura** del curso en línea

Correo electrónico

El correo electrónico es uno de los servicios de red más populares. Con su simplicidad y velocidad, el correo electrónico ha revolucionado la manera de comunicarse. No obstante, para ejecutarse en una computadora o en otro dispositivo final, el correo electrónico requiere de diversos servicios y aplicaciones. Dos protocolos comunes de la capa de aplicación son el Protocolo de oficina de correos (POP, Post Office Protocol) y el Protocolo simple de transferencia de correo (SMTP, Simple Mail Transfer Protocol).

Procesos del cliente de correo electrónico

Los usuarios de correo electrónico generalmente acceden al servicio de correo electrónico utilizando una aplicación denominada cliente de correo electrónico. El cliente de correo electrónico permite a los usuarios crear y enviar mensajes; luego coloca los mensajes recibidos en el buzón del usuario.

Procesos del servidor de correo electrónico

El servidor de correo electrónico también transfiere y entrega correo al cliente de correo electrónico.

Si bien un solo correo electrónico no genera tráfico importante, es posible transmitir correos electrónicos masivos que inundan la red o los servidores con tráfico.

Refiera a la **Figura** del curso en línea

Admisión de aplicaciones de correo electrónico y transferencia de archivos

Los usuarios esperan acceder inmediatamente a sus correos electrónicos y a los archivos que comparten o actualizan.

Para ayudar a asegurar esta disponibilidad, el diseñador de red sigue los pasos a continuación:

- Asegura los servidores de archivos y correos en una ubicación centralizada, por ejemplo, una granja de servidores.
- Protege la ubicación del acceso no autorizado mediante medidas de seguridad lógicas y físicas.
- Crea redundancia en la granja de servidores para asegurar que no se pierdan todos los archivos si falla un dispositivo.
- Configura rutas redundantes a los servidores.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Analizar el tráfico de la red utilizando NBAR.

4.2.4 Tráfico Web y HTTP

Refiera a la **Figura** del curso en línea

Tráfico Web y HTTP

Protocolo de transferencia de hipertexto (***HTTP***, Hypertext Transfer Protocol) es uno de los protocolos del conjunto de aplicaciones TCP/IP que se desarrolló originariamente para publicar y mostrar páginas Web. En la actualidad se utiliza para sistemas de información distribuida y de colaboración. HTTP se utiliza a través de la World Wide Web para transferir datos. Es uno de los protocolos de aplicación de mayor uso.

HTTP especifica un protocolo de respuesta/solicitud entre un cliente, generalmente un explorador Web, y un servidor.

Cuando un cliente envía un mensaje de solicitud a un servidor, el protocolo HTTP define los tipos de mensajes utilizados por el cliente. El protocolo también especifica los tipos de mensajes que el servidor utiliza para responder.

Este proceso parece ser una consideración menor en el proceso de diseño. Sin embargo, si el servidor al que se accede se utiliza para e-commerce o para almacenar información del cliente, los problemas de redundancia y seguridad adquieren aún mayor importancia.

Refiera a la **Figura** del curso en línea

Medios de red

Para admitir el tráfico Web y HTTP, es necesario contar con dispositivos de Capa 3 que puedan controlar los flujos de tráfico externo e interno. En una auditoría de red, el tráfico entrante debe considerarse parte de la prueba básica de red.

Redundancia

Los servidores generalmente tienen fuentes de energía y componentes redundantes. Pueden estar equipados con dos o más NIC conectadas a switches separados.

Seguridad

Las funciones de seguridad, como las ACL, los firewalls y los IDS, también se utilizan para evitar que el tráfico no autorizado entre o salga de las redes protegidas. Al igual que con los demás servidores de aplicación, el servidor HTTP debe estar ubicado en el ISP o en la granja de servidores centralizada para la redundancia y seguridad física incorporada.

4.2.5 Servicios de dominio de Microsoft

Refiera a la **Figura** del curso en línea

El estadio utiliza los servicios Active Directory de Microsoft. Por lo tanto, el diseñador de red debe considerar las comunicaciones de servidor a cliente y de servidor a servidor. Los servidores de Microsoft admiten diferentes tipos de servicios que se basan en las comunicaciones de alta velocidad entre los mismos servidores. Estos servicios, como la duplicación de Active Directory, deben considerarse al reubicar servidores en un nuevo diseño de red.

Puertos utilizados por los servicios de dominio de Microsoft

Los clientes y servidores de Microsoft se comunican entre sí utilizando un conjunto de puertos TCP y UDP. Estos puertos se utilizan para varios servicios de Microsoft, entre ellos la autenticación y la autorización. Muchas servicios específicos de Microsoft generan paquetes de broadcast locales en estos puertos, al igual que solicitudes unicast. Entre los puertos TCP y UDP comunes que deben abrirse para que los servicios de dominio de Microsoft funcionen correctamente se incluyen:

UDP 53: servicios DNS

UDP 67: DHCP

UDP 123: servicio de hora de Windows

TCP 135: llamada de procedimiento remoto (RPC, Remote Procedure Call)

UDP 137: resolución de nombres NetBIOS

UDP 138: servicio de datagrama NetBIOS

TCP 139: servicio de sesión NetBIOS

TCP 389 y UDP 389: servicio LDAP

TCP 445: bloques de mensajes del servidor (SMB, Server Message Blocks)

TCP 1433: SQL de Microsoft por TCP

Active Directory y DNS

Cuando se instala un servidor Microsoft Windows 2003 en una red, existe una integración muy estrecha entre los servicios Active Directory y DNS. Active Directory requiere que DNS ubique controladores de dominio que proporcionan servicios de autorización y autenticación. Los controladores de dominio de Windows 2003 también deben ser servidores DNS. Este servicio DNS puede proporcionar el DNS principal para una organización o agregarse a los servicios DNS de Internet que se encuentran en los servidores que no son de Windows. Las pautas de diseño de Microsoft también recomiendan que DCHP esté integrado con DNS. Esto asegura la creación de una entrada simultánea en el archivo DNS cuando una PC o un dispositivo recibe una dirección IP a través de DHCP.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

4.3 Presentación de Calidad de servicio (QoS)

4.3.1 ¿Qué es QoS y por qué es necesaria?

Refiera a la **Figura** del curso en línea

Calidad de servicio (***QoS***, Quality of Service) se refiere a la capacidad de una red de proporcionar servicio preferencial al tráfico de la red seleccionado. El objetivo principal de QoS es proporcionar

prioridad, incluyendo ancho de banda dedicado, latencia y fluctuación controladas y menor pérdida de paquetes.

Al crear las políticas de QoS para una organización, es importante enfocarse en el tipo de tráfico que necesita tratamiento preferencial. Los diseñadores de red deben considerar de qué manera los problemas de QoS afectan no sólo a los dispositivos de una red, sino también a las aplicaciones que utilizan la red.

Los usuarios perciben la calidad del servicio según dos criterios:

- La velocidad con la que la red reacciona a sus solicitudes
- La disponibilidad de las aplicaciones que desean usar

QoS permite controlar estos aspectos para los flujos de tráfico dentro de la infraestructura de la red y para las aplicaciones que utilizan la red.

Refiera a la **Figura** del curso en línea

Algunos de los dispositivos Cisco, como los routers, cuentan con mecanismos de QoS incorporados.

Algunas aplicaciones son extremadamente sensibles a los requisitos de ancho de banda, los retardos de paquetes, la fluctuación de la red y la posible pérdida de paquetes. Estas aplicaciones incluyen streaming video y telefonía IP en tiempo real.

Requisitos de la telefonía IP

Los requisitos de la telefonía IP ilustran muchos de los problemas de las aplicaciones en tiempo real en una red convergente. El tráfico de voz requiere más que una conexión simple entre los usuarios. La calidad de las transmisiones es sumamente importante. Cuando se producen retardos, las voces se quiebran y las palabras se distorsionan.

Para evitar una calidad de transmisión inferior, la telefonía IP requiere la aplicación de mecanismos de QoS. Los paquetes de voz no deben tener un retardo de una vía mayor que 150 ms. En la implementación de soluciones de telefonía IP es esencial que los paquetes de voz tengan una latencia y fluctuación baja en cada salto a lo largo de una ruta determinada.

Requisitos de streaming video

Streaming video es una señal de video que generalmente se envía desde archivos pregrabados. Puede distribuirse en un broadcast en vivo al convertir el video en una señal digital comprimida y luego se transmite mediante un servidor Web especial. Estos medios de stream se envían como multicast para que varios usuarios puedan ver el stream al mismo tiempo.

En una red sin QoS, todos los paquetes reciben el mismo tratamiento y las aplicaciones en tiempo real se ven afectadas.

En realidad, QoS no genera mayor ancho de banda. En cambio, prioriza el uso del ancho de banda para respaldar las aplicaciones, como la telefonía IP, que más lo necesitan. Para lograrlo, QoS utiliza colas de tráfico para ayudar a administrar el tráfico de prioridad en las redes convergentes.

4.3.2 Colas de tráfico

Tráfico de datos y voz

Refiera a la **Figura** del curso en línea

En una red convergente, el tráfico de voz constante y en paquetes pequeños compite con los flujos de datos irregulares más grandes de las actualizaciones del servidor y las transferencias de archivos. Si

bien los paquetes que a menudo transportan tráfico de voz en una red convergente son pequeños, los retardos que se producen mientras atraviesan la red provocan una calidad de voz inferior.

Los datos de las aplicaciones en tiempo real, como la telefonía IP, deben procesarse con la misma velocidad con la que se envían. Además, no hay tiempo para retransmitir paquetes con errores. Por lo tanto, VoIP utiliza UDP como un protocolo de transporte de máximo esfuerzo.

En cambio, los paquetes que transportan datos de transferencia de archivos, por lo general, son grandes. Estos paquetes utilizan funciones de retransmisión y verificación de errores de TCP para sobrevivir a retardos y descartes de paquetes.

Es posible retransmitir parte de un archivo de datos descartado, pero no es factible retransmitir parte de una conversación de voz. Por esta razón, el tráfico de video y voz, que es esencial y vulnerable a retardos, debe tener prioridad sobre el tráfico de datos.

Mecanismos de QoS

Se deben aplicar mecanismos para proporcionar prioridad de QoS. Las prioridades para el tráfico pueden ser: superior, media, normal o inferior. Las colas de tráfico son sólo uno de los mecanismos de QoS disponibles para priorizar el tráfico en la red. Las colas de tráfico permiten proporcionar servicios garantizados, predecibles y seguros. Incluso una interrupción breve en una red convergente puede perjudicar seriamente las operaciones empresariales.

Refiera a la **Figura** del curso en línea

Colas de hardware y software

Las colas se utilizan para administrar flujo de tráfico con QoS. Las colas de hardware almacenan el tráfico tal como se recibe y envían paquetes en la secuencia recibida según el método de "el primero que llega es el primero que se atiende". La cola de hardware a menudo se denomina cola de transmisión o ***TxQ***. En esta cola física, los paquetes esperan ser enviados según el orden de prioridad.

Las colas de software permiten el envío de paquetes según el orden de prioridad establecido por el diseñador de red o el administrador. Las colas se basan en los requisitos de QoS. Las colas de prioridad (***PQ***, Priority Queuing) y las colas personalizadas (***CQ***, Custom Queuing) son ejemplos de colas de software.

Implementación de QoS en colas de tráfico

Para implementar QoS en una red, el diseñador cumple con tres pasos básicos para garantizar la prioridad adecuada del tráfico:

Paso 1: Identificar los requisitos de tráfico

Determinar los requisitos de QoS necesarios para los diferentes tipos de tráfico como la voz, las aplicaciones esenciales y el tipo de tráfico de prioridad inferior que puede marcarse como tipo de máximo esfuerzo.

Paso 2: Definir las clases de tráfico

Luego de identificar el tráfico, se puede colocar en las clases correspondientes, como el tráfico de voz, que tiene la máxima prioridad, seguido de las aplicaciones esenciales. El resto del tráfico puede recibir prioridad normal o inferior según el propósito de los datos. Los paquetes se marcan para indicar la clase a la que pertenecen.

Paso 3: Definir las políticas de QoS

El último paso es definir las ***políticas de calidad de servicio*** para aplicar a cada clase. Estas políticas incluyen las reglas y colas de tráfico planificadas para administrar la congestión.

4.3.3 Prioridades y administración de tráfico

Refiera a la **Figura** del curso en línea

Existen muchos métodos disponibles para administrar el tráfico de una red. Uno de los métodos es las colas de prioridad (***PQ***, Priority Queuing). Como parte de la implementación de QoS en una red, las colas de prioridad clasifican el tráfico en prioridad superior, media, normal o inferior. Por lo tanto, las colas de prioridad pueden aplicarse a estas clases de QoS.

Las colas de prioridad son útiles para los protocolos esenciales que son vulnerables a retardos. PQ establece cuatro colas de interfaz de salida: superior, media, normal e inferior. Cada una representa un nivel diferente de prioridad. Estas colas son configurables para las siguientes características:

- Tipo de cola
- Asignación de tráfico
- Tamaño

El tráfico entrante se clasifica, se marca para indicar su clase y se envía.

El tráfico se asigna a las diferentes colas según las políticas de QoS definidas en una lista de prioridad. Estas políticas pueden basarse en el protocolo, el número de puerto u otros criterios establecidos para el tipo de tráfico designado. Representan un conjunto de filtros que separan diferentes tipos de tráfico en las cuatro colas en función de las clases.

Refiera a la **Figura** del curso en línea

Cisco incorpora herramientas para contribuir a la configuración de QoS. Una de esas herramientas es AutoQoS y se encuentra disponible como parte del software IOS de Cisco.

Cisco AutoQoS proporciona una interfaz de línea de comandos (CLI, Command Line Interface) inteligente y simple. Esta CLI habilita la QoS de la WAN y la LAN para VoIP en routers y switches Cisco.

AutoQoS incorpora las mejores prácticas de Cisco para implementar QoS y facilita a los clientes la configuración de sus redes para admitir tráfico de prioridad superior, como la voz o el video.

Cisco AutoQoS puede disminuir el costo de implementación y el plazo hasta en dos tercios, en comparación con el método manual.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Clasificar el tráfico según las situaciones dadas y específicas del estudio de caso del estadio.

4.3.4 ¿Dónde se puede implementar QoS?

Refiera a la **Figura** del curso en línea

Al configurar las funciones de QoS, el administrador de red puede seleccionar el tráfico de red específico, priorizarlo según su importancia relativa, y utilizar técnicas de administración de la congestión para proporcionar tratamiento preferencial. QoS puede implementarse en las capas de núcleo, distribución y acceso de una red.

Dispositivos de Capa 2

Los switches de Capa 2 en la capa de acceso pueden admitir QoS según la clase de servicio (CoS) IEEE 802.1p. QoS del switch de Capa 2 utiliza la clasificación y programación para priorizar el envío de tramas del switch a la red.

Dispositivos de Capa 3

Los dispositivos de Capa 3 pueden admitir QoS según la interfaz física, las direcciones IP, los números de puerto lógico y los bits de QoS en el paquete IP. Se debe admitir QoS en los dispositivos de las capa de distribución y núcleo en ambas direcciones del flujo de tráfico.

Clasificación y marcación

La clasificación es el proceso mediante el cual se agrupa el tráfico. Las clasificaciones se realizan según la forma en que se marque el trafico o por protocolo. El tráfico puede marcarse según la clase de servicio de Capa 2, una prioridad IP o un valor del punto de código de servicios diferenciados (***DSCP***, Differentiated Services Code Point):

- La clase de servicio (CoS) representa los 3 primeros bits de una etiqueta VLAN 802.1q.
- La prioridad IP representa los 3 primeros bits del byte del tipo de servicio (***ToS***, Type of Service) en el encabezado IP.
- El router o switch pueden asignar el DSCP. Representa los 6 primeros bits en el byte de ToS en el encabezado.

La clasificación y marcación permiten dividir el tráfico en varios niveles de prioridad o clases de servicio.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Configurar una cola de prioridad para marcar paquetes. Utilice NetFlow para ver las marcas de paquetes. Cree una lista de posibles áreas para la inclusión de redundancia y QoS.

4.4 Examen de las opciones de video y voz

4.4.1 Consideraciones de la red convergente

Refiera a la **Figura** del curso en línea

Las redes modernas pueden admitir servicios convergentes donde el tráfico de video y voz se fusione con el tráfico de datos. Un ejemplo típico es la red del estadio.

Administración de redes convergentes

Los métodos de control para el tráfico de video y voz en las redes convergentes son diferentes de los métodos de control para otros tráficos, como el tráfico basado en la Web (HTTP).

Calidad de servicio (QoS) en redes convergentes

Todas las redes funcionan mejor cuando QoS controla lo siguiente:

- Retardo y fluctuación
- Provisión de ancho de banda
- Parámetros de pérdida de paquetes

Las redes convergentes necesitan un rendimiento sólido y funciones de seguridad para administrar los requisitos conflictivos del tráfico. Por este motivo, los mecanismos de QoS son obligatorios.

4.4.2 Requisitos de una solución de telefonía IP

Uno de los requisitos técnicos de la red del estadio es actualizar una solución de telefonía IP.

Refiera a la **Figura** del curso en línea

Consideraciones de diseño de la telefonía IP

El diseño de red propuesto debe incluir:

- Planificación de capacidad y potencia
- Identificación de los flujos de tráfico disputados
- Selección de los componentes para la solución de telefonía IP

Los componentes de una solución de telefonía IP pueden incluir:

- Teléfonos IP
- ***Gateway***
- Unidad de control multipunto (***MCU***, Multipoint control unit)
- ***Agente de llamadas***
- Servidores de aplicación
- Punto terminal de video
- Teléfono de software

Otros componentes, como las aplicaciones de voz de software y los sistemas de respuesta de voz interactiva (***IVR***, interactive voice response) proporcionan servicios adicionales para satisfacer las necesidades de los sitios empresariales.

Refiera a la **Figura** del curso en línea

Aislamiento del tráfico

Si la PC del cliente y el teléfono IP se encuentran en la misma VLAN, cada una intentará utilizar el ancho de banda disponible sin considerar el otro dispositivo. El método más simple para evitar un conflicto es utilizar VLAN separadas para el tráfico de telefonía IP y el tráfico de datos.

Beneficios de las VLAN separadas

La utilización de VLAN separadas brinda los siguientes beneficios:

- QoS puede priorizar el tráfico de telefonía IP a medida que atraviesa la red.
- Los administradores de red pueden identificar y resolver problemas de red de manera más sencilla cuando los teléfonos se encuentran en VLAN y subredes IP separadas.

La actualización propuesta para la red del estadio, incluso la solución de telefonía IP, requiere del desarrollo de una estructura VLAN y un esquema de direccionamiento IP más eficientes. El diseñador de red debe agregar esta información al documento de requisitos de diseño.

La administración del estadio desea reemplazar su sistema telefónico digital con telefonía IP.

Refiera a la **Figura** del curso en línea

Telefonía tradicional

Por lo general, los sistemas telefónicos tradicionales para empresas se crean sobre una unidad de control central denominada central telefónica privada (***PBX***, Private Branch Exchange). Las PBX transmiten llamadas de voz mediante líneas digitales o analógicas, según el tipo de dispositivo. Por ejemplo, una máquina de fax o un teléfono analógico utilizan una línea analógica y un teléfono de escritorio digital utiliza una línea digital. En la telefonía tradicional, la dirección física del teléfono depende del cable al cual está conectado. Por lo tanto, para agregar, trasladar o cambiar de teléfono, es necesario realizar una cantidad considerable de configuraciones manuales. La mayoría de las empresas tienen una infraestructura de cableado separada para admitir la red telefónica, además de la infraestructura que admite la red de datos.

La compañía del estadio cuenta con un sistema PBX digital que opera a través de una infraestructura separada.

VoIP

Cisco utiliza el término VoIP cuando usa routers con capacidad de voz para convertir la voz analógica de los teléfonos tradicionales en paquetes IP y enrutar dichos paquetes entre las ubicaciones. En la industria de TI, VoIP se utiliza indistintamente con la telefonía IP. Mediante VoIP,

PBX se conecta a un router con capacidad de voz. No se conecta a ***PSTN*** o a otra PBX. Las empresas utilizan VoIP para reducir costos al consolidar enlaces WAN, disminuir los cargos por llamadas de larga distancia y reducir la cantidad de personal de soporte.

Refiera a la **Figura** del curso en línea

Telefonía IP

La telefonía IP reemplaza los teléfonos tradicionales con los teléfonos IP y utiliza el Administrador de comunicaciones unificadas de Cisco, un servidor que se usa para la señalización y el control de llamadas. La telefonía IP posee las siguientes funciones:

- Integra las aplicaciones de voz y mensajería de voz que se conectan a través de la red IP y no mediante sistemas digitales o analógicos.
- Utiliza un teléfono IP para realizar la conversión de voz a IP.
- Crea relaciones punto a punto entre los teléfonos que participan en una conversación en lugar de enrutar llamadas de manera centralizada como lo hace PBX.

El diseñador de red y el cliente pueden incorporar telefonía IP o VoIP en una red de datos existente, creando así una red convergente.

La compañía del estadio esperar obtener los siguientes beneficios de la telefonía IP:

- Administración simplificada de traslados, agregaciones y cambios de oficina
- Aplicaciones adicionales, como directorios y páginas Web, al sistema telefónico
- Reducción de costos de administrar las infraestructuras separadas

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de pantalla completa

4.4.3 Video: en vivo o a pedido

Refiera a la **Figura** del curso en línea

El ancho de banda mayor permite a los usuarios de la red contar con audio y video en sus sistemas de computación. El video puede verse como video en vivo o a pedido (***VoD***, Video on Demand).

Video en vivo

El video en vivo o ***streaming video*** permite a los usuarios ver el contenido antes de que todos los paquetes de medios se encuentren en su sistema de computación. Los archivos de streaming media no tienen período de espera para la visualización; se encuentran disponibles al instante como un stream continuo de paquetes de datos. Streaming video elimina la necesidad de almacenar archivos grandes de medios o de asignar espacio de almacenamiento para los archivos antes de reproducirlos. A menudo, se envía una señal de video en vivo utilizando paquetes multicast para varios usuarios al mismo tiempo.

VoD

Mediante VoD, los usuarios pueden transmitir o descargar todo el contenido a la caché de su computadora antes de verlo. La descarga del archivo de video completo antes de verlo también se denomina almacenamiento y envío. Este método minimiza la carga en los recursos del sistema. La instalación de un servidor para dirigir streaming media a la caché de una computadora permite a los usuarios retener el contenido y verlo más tarde. VoD se envía utilizando paquetes unicast al usuario específico que solicita el video.

La administración del estadio requiere streaming video y VoD. Esto genera tráfico adicional en la red. Si se ubican los servidores para el almacenamiento de video dentro de una granja de servidores, se facilita la administración de la resolución de problemas, la redundancia y la seguridad.

Refiera al **Gráfico Interactivo** del curso en línea

Pantalla completa

4.4.4 Soporte de voz y video para trabajadores remotos

Refiera a la **Figura** del curso en línea

Los desarrollos tecnológicos permiten una mayor flexibilidad para los trabajadores en cuanto al modo y lugar de trabajo. Por ejemplo, los trabajadores en el estadio se conectan al sitio central desde varios sitios remotos.

Para aprovechar las comunicaciones y los recursos del sitio central, un trabajador a distancia, una sucursal o un usuario móvil normalmente tienen al menos una conexión WAN al sitio central. Los requisitos de ancho de banda para la conexión WAN dependen del tipo de recursos de red que necesitan los usuarios para desempeñarse en el trabajo. Si los trabajadores remotos son parte de la red de telefonía IP, posiblemente sea necesario ubicar un sistema administrador de llamadas de manera remota. El diseñador de red considera si es necesario que los trabajadores remotos tengan acceso a los recursos de video en forma simultánea. Este acceso afecta el ancho de banda. Por ejemplo, streaming video puede utilizarse para una reunión empresarial. Estas decisiones de diseño requieren también la evaluación del ancho de banda en la conexión WAN del sitio central.

¿Enlace permanente o a pedido?

El diseñador de red decide si es mejor utilizar enlaces permanentes con el sitio central o a pedido. El diseñador trabaja con el cliente para considerar los requisitos de costo, seguridad y disponibilidad.

Refiera a la **Figura** del curso en línea

Una conexión de Internet de alta velocidad es una solución útil para los trabajadores a distancia. Es fácil de configurar en oficinas remotas y también se encuentra disponible en muchos hoteles. La administración del estadio planea proporcionar conexión de Internet utilizando puntos de acceso inalámbricos en los palcos de lujo y en el restaurante del estadio.

A veces, las conexiones dial-up asíncronas son la única solución de acceso remoto disponible para los viajeros. Los empleados que viajan pueden utilizar una PC con módem y la red telefónica existente para conectarse a la compañía.

Las conexiones WAN en los sitios de los empleados a distancia pueden incluir las siguientes funciones:

- Dial-up asíncrona
- BRI ISDN
- Módems por cable
- DSL
- Conexión inalámbrica y satelital
- VPN

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Investigar el impacto del tráfico multicast de streaming video en una red.

4.5 Documentación del flujo de tráfico y aplicaciones

4.5.1 ¿Qué es un flujo de tráfico?

Flujo de tráfico

Refiera a la **Figura** del curso en línea

El flujo de tráfico en una red es similar al flujo de tráfico en las calles de una ciudad. Así como los vehículos se trasladan de un lugar a otro a través de la ciudad, el tráfico generado por las aplicaciones se traslada de una ubicación a otra de la red.

Un vehículo en la calle viaja desde un punto de partida hacia un destino. De manera similar, un flujo de tráfico creado por una aplicación viaja como un stream de paquetes unidireccional entre un origen y un destino. Por lo general, la dirección IP de una capa de red define la ruta. En función de QoS y las políticas configuradas en la red, la ruta puede estar influenciada por otra información, como los números de puerto de destino y origen de la capa de transporte. Por ejemplo, un host envía una solicitud de archivo a un servidor en un flujo. El servidor procesa la solicitud y devuelve el archivo al host en otro flujo.

Control de tráfico

Sin ningún tipo de control de tráfico, como por ejemplo las señales de tránsito o las rutas alternativas para mantener el flujo, el tráfico en las calles se congestiona. Las redes también necesitan una forma de controlar los flujos de tráfico. Los mecanismos de QoS están diseñados para asegurar un flujo ágil del tráfico de aplicaciones en la red.

Refiera a la **Figura** del curso en línea

Flujos de tráfico de aplicaciones

El flujo de tráfico de aplicaciones dentro y fuera de una porción de la red puede ser mínimo algunas veces y otras considerablemente mayor. Por ejemplo, en el estadio deportivo, el tráfico en las primeras horas de la mañana puede incluir solicitudes de correo electrónico, acceso a Internet y cargas de archivos a los servidores del estadio. El tráfico de la tarde puede incluir VoIP, correo electrónico, transferencias de archivos y procesos de transacciones de la venta de entradas.

Si el diseñador de red no calcula correctamente el volumen de tráfico de las aplicaciones durante el diseño inicial de la red del estadio, todas las aplicaciones pueden sufrir rendimiento degradado y congestión de la red. Los clientes en los puestos de venta y quioscos para la compra de entradas pueden experimentar retardos significativos o incluso la imposibilidad de acceder a las aplicaciones. La satisfacción del cliente disminuiría.

Para lograr visualizar el tráfico actual y futuro de la red, el diseñador crea un diagrama de flujos de tráfico. El primer paso es identificar las aplicaciones proyectadas en la red. Esta información se recopila de las siguientes fuentes:

- Información del cliente
- Auditoría de la red
- Análisis de tráfico

El diseñador documenta estas aplicaciones y el hardware relacionado en un diagrama de red.

Refiera a la **Figura** del curso en línea

Es sumamente importante identificar los flujos de tráfico entre los hosts. El diseñador de red utiliza los contenidos de diagramas físicos o lógicos para planificar el diseño a fin de incorporar el tráfico de aplicaciones existentes y nuevas.

El diseñador de red generalmente utiliza un programa de diseño, como ***MS Visio***, para crear un diagrama que muestre las aplicaciones identificadas y la topología lógica de la red.

Luego de crear el diagrama de aplicaciones, dispositivos y flujo de tráfico, el diseñador analiza el diseño propuesto e identifica las áreas donde se puede mejorar la red.

A partir del diagrama lógico, el diseñador identifica las posibles áreas de congestión. Luego, determina el equipo necesario para manejar el tráfico que fluye de host a host y de host al servidor.

En el estadio, el diagrama de topología lógica muestra los flujos de tráfico de host a host y de host a los servidores. La conexión de los dispositivos también muestra las aplicaciones que se utilizarán. El tráfico generado entre los hosts es relativamente menor en comparación con el tráfico generado de los hosts hacia los servidores.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Identificar los flujos de tráfico de CompañíaCinematográfica. Utilice NetFlow para identificar las aplicaciones y el destino del tráfico.

4.5.2 Diagramación de flujos de tráfico interno (Intranet)

Refiera a la **Figura** del curso en línea

La red del estadio brinda servicios a una organización compleja que tiene muchas áreas operativas. Las oficinas de administración, los servidores, los proveedores y las oficinas de venta de entradas son parte de la red más grande.

Cada LAN dentro del estadio manipula el tráfico que se envía de host a host y del host al servidor. Las transferencias de archivo generales de host a host y el tráfico de correo electrónico no consumen gran cantidad de ancho de banda. Sin embargo, las creación diaria de copias de seguridad en el servidor consumen gran cantidad de ancho de banda y necesitan ser analizadas durante la fase de diseño.

Todos los flujos de tráfico, tanto desde las redes internas como externas, deben evaluarse detalladamente al diseñar una nueva red o al proponer actualizaciones para una red existente. Esta evaluación presenta desafíos únicos para el diseñador de red:

- El tráfico dentro de la red interna es fácil de identificar. Este tráfico puede utilizarse para calcular la utilización de la red.
- El tráfico desde la fuentes externas es difícil de describir. El diseñador necesita calcular los requisitos de ancho de banda para los flujos de tráfico externo.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar NetFlow para crear un diagrama del flujo de tráfico de host a host y del host al servidor dentro de un segmento de la LAN de CompañíaCinematográfica.

4.5.3 Diagramación de flujos de tráfico con los sitios remotos

Refiera a la **Figura** del curso en línea

Luego de describir y diagramar todas las secciones de la LAN interna, el diseñador de red se enfoca en los sitios remotos y las VPN.

La cantidad de tráfico que se envía o se recibe de un sitio remoto puede ser menor. En la red del estadio, los flujos de tráfico pueden ser menores, pero son principalmente procesos de transacción que se envían de la oficina de venta de entradas a los servidores que se encuentran en el estadio. Es importante identificar los flujos para fines de seguridad, redundancia y QoS, ya que estas aplicaciones son esenciales.

Como ocurre con la topología LAN, es necesario identificar los dispositivos remotos que generan tráfico en la red. Todos los switches y routers que se utilizan para conectar los sitios remotos al estadio son parte de la ruta que sigue el tráfico de aplicaciones.

El diseñador de red debe calcular la cantidad de tráfico que fluye desde los sitios remotos como parte de los flujos de tráfico externo a la red del estadio. El diseñador también debe determinar si las ACL o firewalls interferirán con el flujo de tráfico adecuado.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar NetFlow para crear un diagrama del flujo de tráfico desde y hacia los sitios remotos de CompañíaCinematográfica.

4.5.4 Diagramación de flujos de tráfico externo

Refiera a la **Figura** del curso en línea

Si bien la mayoría del tráfico en la red existente del estadio es interno, el diseñador de red debe considerar el tráfico externo destinado a Internet.

Es imposible diagramar Internet, teniendo en cuenta la cantidad de dispositivos conectados a esta red. Sin embargo, es posible determinar lo siguiente:

- Los flujos de tráfico saliente destinados a Internet. Un ejemplo de tráfico saliente en la red del estadio serían los usuarios en el estadio que solicitan acceso a los recursos externos, como las noticias deportivas en línea.
- El tráfico entrante fluye desde Internet hacia los servicios prestados a nivel local. Un ejemplo de tráfico entrante serían los clientes que al comprar entradas en línea necesitan acceder a los servidores internos para procesar la compra.

Al determinar los flujos de tráfico relacionados con Internet, ya sean internos o externos, el diseñador puede evaluar la necesidad de obtener redundancia y seguridad para facilitar el tráfico que se genera.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar NetFlow para crear un diagrama de los flujos de tráfico externo de CompañíaCinematográfica.

4.5.5 Diagramación de flujos de tráfico extranet

Refiera a la **Figura** del curso en línea

El estadio cuenta con un sitio remoto y un proveedor que tiene permiso para acceder a la red interna a través de las VPN. Estas VPN permiten el acceso a la internetwork del estadio a través de conexiones encriptadas y seguras. El estadio también cuenta con un servidor de e-commerce basado en la Web que permite a los clientes comprar entradas. Este servidor está protegido con ***SSL***.

Los clientes y el proveedor de confianza utilizan IPSec para asegurar los flujos de tráfico al interior de la red del estadio.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar NetFlow para crear un diagrama de los flujos de tráfico extranet de CompañíaCinematográfica.

Resumen del capítulo

Examen del capítulo

Vaya al curso en línea y complete la prueba

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 5

Creación de diseño de red

Introducción

Refiera a la **Figura** del curso en línea

5.1 Análisis de los requisitos

5.1.1 Análisis de los objetivos comerciales y los requisitos técnicos

Refiera a la **Figura** del curso en línea

El diseño de la actualización de red del estadio inicia sólo después de que se reúnen todos los requisitos y de que se analiza la red existente.

Primero, el diseñador de red considera los objetivos comerciales priorizados. Al comienzo del proceso PPDIOO, el diseñador creó el documento de Requisitos del diseño que enumera los objetivos comerciales así como también los requisitos técnicos que los respaldan. Resulta crítico para el éxito del proyecto que todos los objetivos comerciales se incluyan en el nuevo diseño.

Determinar cómo diseñar una red para cumplir con los objetivos comerciales es un proceso de varias etapas. El diseñador generalmente sigue estos pasos:

Paso 1: Enumere los objetivos comerciales que el nuevo diseño debe cumplir.

Paso 2: Determine qué cambios o adiciones son necesarios para que la empresa cumpla con sus objetivos.

Paso 3: Decida qué requisitos técnicos son necesarios para implementar cada cambio.

Paso 4: Determine la manera en la que el diseño puede cumplir con cada uno de los requisitos técnicos.

Paso 5: Decida qué elementos del diseño deben estar presentes en el diseño final.

Al seguir estos pasos para cada uno de los objetivos comerciales, el diseñador determina qué debe incluirse en el diseño de la red.

Refiera a la **Figura** del curso en línea

Manejo de restricciones

El documento de los Requisitos del diseño incluye una lista de restricciones. Normalmente, cuando las restricciones afectan el diseño se deben hacer concesiones. El diseñador de red explora todas las alternativas posibles y selecciona las mejores para incluir en el diseño.

Realización de compensaciones

Una compensación es un intercambio de un beneficio o ventaja por otro beneficio considerado más deseable. Las restricciones en el diseño de la red suelen forzar compensaciones entre el diseño ideal y un diseño que sea realizable de manera realista. Son comunes las compensaciones entre los beneficios de una solución ideal y la realidad de las restricciones en el tiempo o costo. La tarea del diseñador es minimizar los efectos que estas compensaciones tienen sobre los principales objetivos de escalabilidad, disponibilidad, seguridad y facilidad de administración.

Un ejemplo de una compensación en el diseño de red del estadio es un límite en el presupuesto que evita la conexión a un proveedor de servicios de Internet (ISP) secundario. Debido a este límite se debe diseñar una estrategia alternativa para cumplir con los requisitos de disponibilidad de los servidores de e-commerce. El diseñador recomienda que los servidores redundantes adicionales sean ***coubicados*** en el sitio del ISP para proporcionar la disponibilidad necesaria en el caso de una pérdida de conectividad con el ISP.

Cada vez que se deba realizar una compensación durante la fase de diseño, el diseñador debe asegurar que el cliente está informado y que está de acuerdo con el compromiso.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de página completa: MCMA

Identificar los elementos del diseño que puedan verse afectados por las restricciones del diseño.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad de laboratorio

Analizar cómo las restricciones que se imponen a la red de CompañíaCinematográfica afectan el proceso del diseño.

5.1.2 Requisitos para la escalabilidad

Refiera a la **Figura** del curso en línea

La administración del estadio anticipa un importante crecimiento en ciertas áreas de la red. No esperan que la cantidad de conexiones con cable aumenten rápidamente. La administración del estadio planifica agregar como mínimo dos nuevos sitios para oficinas remotas. Esta expansión aumenta la cantidad de usuarios en un 50%, para alcanzar aproximadamente 750 usuarios.

Son importantes los requisitos de escalabilidad que se recibieron de la administración del estadio:

- El 50% de incremento en la cantidad total de usuarios (LAN y WAN)
- El 75% de incremento en la cantidad de usuarios inalámbricos
- El 75% de incremento en la cantidad de transacciones en línea a través de los servidores e-commerce del estadio
- El 100% de incremento en la cantidad de sitios remotos
- Aumento del número de teléfonos IP y la incorporación de la red de video sumando 350 dispositivos finales

El diseñador de red cree que la administración del estadio está subestimando demasiado la necesidad del respaldo inalámbrico. La administración del estadio estima un incremento de sólo 75% sobre los 40 dispositivos inalámbricos actualmente conectados. El diseñador anticipa que se necesita una cantidad considerable de dispositivos adicionales en el diseño inicial para respaldar las áreas de cobertura solicitadas. Además, el diseñador recomienda siempre permitir el 20% de crecimiento. El diseñador toma nota para tratar este tema inmediatamente con la administración del estadio.

Refiera a la **Figura** del curso en línea

Para respaldar este rápido crecimiento, el diseñador de red desarrolla una estrategia para permitir que la red aumente en forma efectiva y fácil. En la estrategia se incluyen las siguientes recomendaciones:

- Los módulos de la capa de acceso del diseño que se pueden agregar según sea necesario sin afectar el diseño de las capas núcleo y de distribución.
- Utilice equipo modular expansible o de dispositivos ***agrupados*** que puedan actualizarse fácilmente para incrementar las capacidades.
- Elija routers o switches de capas múltiples para limitar broadcast y filtrar otro tipo de tráfico no deseado en la red.

- Planifique utilizar varios enlaces entre el equipo, ya sea a través de ***EtherChannel*** o de un balanceo de carga de mismo costo para incrementar el ancho de banda.
- Cree una estrategia de dirección IP que sea jerárquica y que admita la creación de resúmenes.
- Cuando sea posible, mantenga las VLAN locales en el armario de cableado.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad

Según la cantidad de AP planificados y una cantidad calculada de 20 dispositivos de datos por AP, ¿cuántos dispositivos inalámbricos puede admitir aproximadamente la red del estadio propuesta?

Refiera a la **actividad de laboratorio** del curso en línea

Actividad de laboratorio

Identificar las estrategias de diseño que cumplen con los requisitos de escalabilidad de la red de CompañíaCinematográfica.

5.1.3 Requisitos para la disponibilidad

Refiera a la **Figura** del curso en línea

En la red del estadio, los sistemas de telefonía IP, e-commerce y seguridad planificados se basan en que la red subyacente esté disponible las 24 horas del día, los 7 días de la semana.

Las transacciones incompletas en el sitio Web pueden hacer que la administración del estadio pierda ingresos. Si no se cuenta con el monitoreo de seguridad, puede peligrar la seguridad de los clientes del estadio. Cuando un sistema de telefonía deja de funcionar, se pierden comunicaciones esenciales.

El diseñador de la red debe desarrollar una estrategia para la disponibilidad que proporcione la protección máxima contra fallas y que no sea demasiado costosa de implementar. Para proporcionar el requisito del tiempo de actividad de casi el 100% para las aplicaciones de red, el diseñador debe implementar características de alta disponibilidad y redundancia en el nuevo diseño.

Refiera a la **Figura** del curso en línea

Disponibilidad para e-commerce

Un sitio Web no confiable puede rápidamente convertirse en un problema de soporte e incluso desalentar a los clientes en la realización de transacciones. Para asegurar la confiabilidad para e-commerce, utilice las siguientes prácticas recomendadas:

- Realice una conexión doble de los servidores en dos switches distintos de la capa de acceso.
- Proporcione conexiones redundantes en la capa de distribución.
- Proporcione servidores DNS secundarios coubicados en el ISP.
- Incluya el monitoreo adicional local y por medio de Internet para los dispositivos que se encuentran en la ruta crítica.
- Cuando sea posible, incluya módulos redundantes y fuentes de energía en los equipos críticos.
- Proporcione un UPS y un respaldo de alimentación con generador.
- Seleccione una estrategia para el protocolo de enrutamiento que asegure una rápida convergencia y un funcionamiento confiable.
- Investigue opciones para proporcionar un proveedor de servicios de Internet (ISP) adicional o conectividad redundante al único ISP.

Sistema de monitoreo de la seguridad

Refiera a la **Figura** del curso en línea

Los servidores que mantienen los archivos de video y el software de administración de seguridad tienen los mismos requisitos de disponibilidad que los servidores de e-commerce. Se necesitan las siguientes medidas adicionales para las cámaras y el equipo de vigilancia:

- Cámaras redundantes en las áreas críticas que estén conectadas a switches individuales para limitar el efecto de una falla de
- Power over Ethernet (***PoE***) en las cámaras, con UPS o respaldo con generador

Sistema de telefonía IP

Aunque la instalación del nuevo sistema de telefonía IP se encuentre fuera del ámbito de este proyecto de diseño de red, es necesario que el diseñador de red considere los requisitos de disponibilidad en el diseño. El diseñador se enfoca en los siguientes requisitos para proporcionar redundancia y alta disponibilidad en los switches de la capa de acceso:

- Implementar la conectividad de Capa 3 entre los dispositivos de la capa de acceso y la capa de distribución cuando sea posible.
- Proporcionar respaldo con UPS y alimentación redundante.
- Crear rutas redundantes desde la capa de acceso a la capa núcleo.
- Reducir el tamaño de los dominios de fallas.
- Cuando sea posible, seleccionar equipo que pueda respaldar componentes redundantes.
- Utilizar un protocolo de enrutamiento convergente rápido, como EIGRP.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad

Describir cómo las distintas estrategias de disponibilidad mejoran la confiabilidad de la red y limitan los efectos de las fallas.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad de laboratorio

Identificar las estrategias disponibles que cumplen con los requisitos de diseño de la red de CompañíaCinematográfica.

5.1.4 Requisitos para el rendimiento de la red

Refiera a la **Figura** del curso en línea

Las redes convergentes, como la red que se está diseñando para el estadio, transportan una combinación de tráfico de video, voz y datos. Cada tipo de tráfico tiene requisitos de servicio únicos.

Las características representativas de las aplicaciones en una red convergente típica incluyen:

- Paquetes de distintos tamaños
- Grupos de protocolos definidos
- Distintas tolerancias al ***retardo*** y a la ***fluctuación de fase***

Algunas veces los requisitos de servicio de una aplicación entran en conflicto con los de otra, lo cual genera problemas de rendimiento. Cuando se produce esta situación, los usuarios frustrados llaman al soporte técnico para informar que la aplicación está lenta.

Incluso los profesionales de TI con experiencia y capacitados tienen problemas para mantener el alto desempeño de la aplicación. Es difícil implementar nuevas aplicaciones y servicios sin alterar los existentes.

En la nueva red del estadio hay tres aplicaciones que tienen requisitos de desempeño específicos que deben considerarse:

- Procesamiento de transacciones
- Monitoreo y distribución de video
- Calidad de voz del teléfono IP

Refiera a la **Figura** del curso en línea

El diseñador de red crea una lista de los objetivos de diseño y las consideraciones que podrían afectar el desempeño de estas aplicaciones de alta prioridad.

Objetivo: Reducir el tiempo de procesamiento de transacciones a menos de 3 segundos.

- Reducir el ***diámetro de la red***.
- Restringir los broadcast y el tráfico no deseado.
- Proporcionar rutas de gran ancho de banda hacia los servidores claves.
- Recomendar almacenamiento adicional de alta velocidad o servidores de contenido.

Objetivo: Proporcionar voz de alta calidad y streaming video.

- Diseñar la estrategia para la clasificación de tráfico y VLAN.
- Mantener cortas las rutas desde el servidor hacia los puntos finales.
- Reducir el número de veces que se procesa o filtra el tráfico.
- Aumentar el ancho de banda del sitio WAN y mejorar la conectividad.
- Determinar la estrategia de QoS y las prioridades del tráfico.
- Identificar las áreas donde se pueden producir cuellos de botella y desplegar una estrategia de QoS.

5.1.5 Requisitos para la seguridad

Refiera a la **Figura** del curso en línea

La seguridad es un área del diseño de red en donde no se deben realizar compensaciones. Aunque es posible que pueda ser necesario encontrar formas menos simplificadas o de menor costo para proporcionar una red segura, nunca es aceptable ignorar la seguridad con el objeto de sumar otras capacidades a la red.

Una evaluación del riesgo de la red identifica las áreas en donde la red es más vulnerable. Las redes que contienen información altamente confidencial o crítica suelen tener consideraciones de seguridad especiales. Las organizaciones realizan evaluaciones de riesgo como parte de su plan de recuperación ante desastres y continuidad general de la empresa.

La mayoría de las redes se benefician con las prácticas estándar recomendadas cuando se trata de implementar la seguridad. Las prácticas de seguridad recomendadas incluyen:

- El uso de firewalls para separar todos los niveles de la red corporativa protegida de otras redes no protegidas, como Internet. Configurar firewalls para monitorear y controlar el tráfico sobre la base de una política de seguridad escrita.
- Crear comunicaciones seguras utilizando las VPN para encriptar la información antes de enviarla a través de una red sin protección o de terceros.
- Prevenir los ataques e intrusiones a la red implementando ***sistemas de prevención de intrusión***. Estos sistemas analizan la red en busca de comportamiento malicioso o dañino y alertan a los administradores de red.

- Controlar las amenazas de Internet utilizando defensas para proteger el contenido y a los usuarios de virus, spyware y correo no deseado.
- Administrar la seguridad en los puntos finales para proteger la red mediante la verificación de la identidad de cada usuario antes de conceder acceso.
- Asegurar que haya medidas de seguridad física para prevenir el acceso no autorizado a las instalaciones y los dispositivos de red.
- Proteger los puntos de acceso inalámbricos e implementar soluciones de administración de inalámbricos.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad de laboratorio

Investigar las distintas opciones de seguridad y efectuar una recomendación utilizando los requisitos de CompañíaCinematográfica.

5.1.6 Cómo se realizan compensaciones en el diseño de red

Refiera a la **Figura** del curso en línea

Se deben tomar algunas decisiones difíciles luego de que el diseñador de red enumera todos los elementos que necesitan estar presentes en el diseño de la actualización del estadio. Desafortunadamente, se pueden diseñar pocas redes sin considerar:

- El costo de la red
- La dificultad de implementación
- Los requisitos de soporte futuros

EstadioCompañía ha colocado algunas restricciones en la actualización de la red que requieren que el diseñador evalúe las distintas opciones de diseño. Es posible que resulte necesario realizar compensaciones en algunas áreas para dar lugar a estas restricciones.

El principal objetivo comercial de EstadioCompañía es mejorar la atmósfera y la seguridad para las miles de personas que asisten al estadio. Las mejoras de la red que afectan directamente la manera en la que la red respalda este objetivo deben ser una de las principales prioridades para el diseñador al momento de realizar compensaciones.

El apoyo a los objetivos comerciales puede llevar a decisiones que eliminen o compliquen otras mejoras necesarias o deseables. Por ejemplo, agregar el acceso inalámbrico para mejorar la experiencia del cliente en las cabinas de lujo y en el restaurante puede disminuir la seguridad del servidor a menos que el acceso del invitado se aísle de la red interna.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad

Evaluar las posibles compensaciones en función de los objetivos comerciales priorizados.

5.2 Selección de la topología de LAN adecuada

5.2.1 Diseño de una topología de la capa de acceso

Refiera a la **Figura** del curso en línea

El diseñador de red está listo para comenzar el diseño de la actualización de la LAN del estadio. La LAN actual es una topología de la red plana sin enlaces redundantes y muy poca seguridad. Este diseño no cumple con los requisitos de la administración del estadio.

Requisitos de la capa de acceso

El diseñador crea la siguiente lista de requisitos de red de la capa de acceso para la nueva red:

- Proporcionar conectividad para los dispositivos de red existentes y agregar acceso inalámbrico y teléfonos IP.
- Crear las VLAN para separar la voz, el monitoreo de vigilancia de seguridad, el acceso inalámbrico y los dispositivos de datos normales.
- Restringir las VLAN a los armarios de cableado, con excepción de la VLAN inalámbrica, para admitir futuros requisitos de roaming.
- Proporcionar enlaces redundantes a la red de la capa de distribución.
- Utilizar los 16 switches 2960 actuales cuando sea posible.
- Proporcionar Power over Ethernet (PoE) a los teléfonos IP y a los puntos de acceso inalámbrico si fuera posible.
- Proporcionar clasificación de QoS y capacidades de marcado.

Refiera a la **Figura** del curso en línea

Un incremento en la cantidad de hosts no siempre necesita de un incremento igual en la cantidad de dispositivos y puertos. Por ejemplo, los teléfonos IP y otros dispositivos incluyen un switch incorporado que permite conectar una PC directamente al teléfono. Este switch reduce el número de puertos que se necesitan en el armario de cableado para conectar los dispositivos adicionales. Si se supone que más del 50% de los teléfonos IP también conectan dispositivos de PC, es posible que no sea necesario agregar un nuevo switch al armario de cableado al agregar más conexiones de datos.

Los teléfonos IP tienen tres puertos:

- El puerto 1 es un puerto externo que se conecta al switch o a otro dispositivo VoIP.
- El puerto 2 es una interfaz 10/100 interna que transporta el tráfico de telefonía IP.
- El puerto 3 es un puerto de acceso externo que se conecta a una PC o a otro dispositivo.

Refiera a la **Figura** del curso en línea

Los 16 switches 2960 existentes se van a utilizar en la capa de acceso para proporcionar al usuario final. El diseñador de red debe asegurar que el switch 2960 es adecuado para la nueva red.

Capacidades del switch 2960

Estos switches son Ethernet 10/100 de ***configuración fija*** con dos puertos uplink 10/100/1000. El 2960 puede cumplir con la mayoría de los siguientes requisitos de la red de la capa de acceso:

- **Escalabilidad**: el 2960 admite la ***agrupación de switches de Cisco***; por lo tanto, se pueden agregar switches nuevos para admitir conectividad adicional.
- **Disponibilidad**: el 2960 es compatible con las fuentes de energía redundantes. La administración redundante de switch está disponible cuando los switches se configuran en un clúster. Se puede configurar dos switches como switches de comando. Si uno falla, el resto del clúster todavía puede funcionar. Las capacidades de marcado y clasificación también están disponibles en este modelo.
- **Seguridad**: están disponibles la seguridad del puerto y otras opciones de seguridad de switch.
- **Facilidad de administración**: los switches admiten el Protocolo simple de administración de red (***SNMP***). Se les puede administrar ***dentro de banda*** y ***fuera de banda***. El 2960 admite el grupo de comandos para el software IOS de Cisco estándar, así como también la configuración de la GUI del asistente de Cisco Network y las herramientas de administración.

Refiera a la **Figura** del curso en línea

Limitaciones del equipo actual

El switch 2960 tiene ciertas limitaciones en el nuevo diseño de red. Los switches 2960 actuales de la red del estadio necesitan transceptores adicionales para admitir los uplink de fibra. Debido a que sólo hay dos conexiones de fibra disponibles en cada armario de cableado, varios switches 2960 deben agruparse para compartir los uplink. El 2960 es un switch de Capa 2; por lo tanto, el diseñador de red está limitado a proporcionar funcionalidad de Capa 2 en la capa de acceso.

Requisitos de alimentación

Aunque el switch 2960 no admite PoE, sí admite la capacidad de VLAN de voz. Es posible que sea necesario utilizar paneles de conexión con alimentación para alimentar los teléfonos IP hasta que en el futuro se cambien los switches.

Las unidades UPS proporcionan energía de respaldo para los switches y los paneles de conexión con alimentación. El diseñador recomienda comprar un generador para proporcionar alimentación a las áreas críticas de la capa de acceso.

El diseñador no especifica cómo se respalda la red inalámbrica en la capa de acceso. Existen otros factores, como la capacidad de roaming, que afectan el diseño de la red inalámbrica. El diseñador sabe que el diseño inalámbrico todavía no está completo.

5.2.2 Diseño de la topología de la capa de distribución

Refiera a la **Figura** del curso en línea

La capa de distribución de la red del estadio es responsable del enrutamiento del tráfico entre las VLAN y de filtrar el tráfico no deseado.

Requisitos de la capa de distribución

El diseñador de la red crea la siguiente lista de requisitos para la capa de distribución de la nueva red:

- Proporcionar componentes redundantes y enlaces para minimizar el efecto de una falla.
- Admitir el enrutamiento de alta densidad. Después de algún tiempo, cada uno de los 16 armarios de cableado del estadio pueden tener más de un uplink a los switches de la capa de distribución.
- Proporcionar las capacidades de filtrado de tráfico.
- Implementar los mecanismos de QoS.
- Proporcionar conectividad de gran ancho de banda.
- Implementar un protocolo de enrutamiento de convergencia rápida.
- Sumar el tráfico y realizar el resumen de ruta.

Los switches de varias capas son una elección adecuada para cumplir con estos requisitos. Proporcionan alta densidad de puerto y admiten las capacidades de enrutamiento necesarias. El diseño de la capa de distribución incluye conectividad para los usuarios de la LAN, la granja de servidores y la distribución de margen empresarial. Se deben comprar seis switches de varias capas para proporcionar el soporte requerido.

Restricciones del diseño

Refiera a la **Figura** del curso en línea

La cantidad limitada de conectividad de fibra hacia los armarios de cableado es la única restricción del diseño que limita la capa de distribución. Los dos pares de fibra que conectan los armarios de cableado limitan la cantidad de switches que se pueden conectar de manera redundante al equipo de la capa de distribución. Como toda la fibra termina en una ubicación central, gran parte del equipo de la capa de distribución debe instalarse en el nuevo centro de datos.

Capacidades del switch de capas múltiples

El uso de los switches de capas múltiples en la capa de distribución cumple con los requisitos técnicos de diseño del estadio:

- **Escalabilidad**: los switches de capas múltiples modulares admiten puertos de cobre y de fibra adicionales. El uso del enrutamiento en la capa de distribución evita muchos problemas de reconfiguración del Protocolo de árbol de expansión (***STP***) de Capa 2. Se pueden agregar ***bloques de switches*** nuevos sin afectar la topología existente.
- **Disponibilidad**: los switches de varias capas de rango medio admiten fuentes de energía redundantes y ventiladores. Más importante aún, admiten módulos de administración redundantes y tecnología de conmutación por error rápida. Si falla un módulo de administración, el módulo secundario lo reemplaza sin que se perciba la pérdida de conectividad. El diseño conmutado de Capa 3 utiliza de la mejor manera los enlaces de red con un balanceo de carga eficiente del tráfico direccionado. Los protocolos de enrutamiento pueden configurarse para que converjan con la rapidez de STP o más rápido aún. El resumen de ruta puede producirse en la capa de distribución reduciendo el impacto de un dispositivo de la capa de acceso o la falla del enlace en el enrutamiento de la capa núcleo.
- **Seguridad**: el filtrado de la lista de acceso, la seguridad del puerto y la función de firewall están disponibles con el switch de varias capas IOS de Cisco. Las características de seguridad adicionales previenen el tráfico de red no deseado o no autorizado.
- **Facilidad de administración**: los switches admiten SNMP. Se les puede administrar dentro y fuera de banda.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad en Packet Tracer

Planificar la interconexión de un bloque de switch de la capa de acceso con conexiones redundantes a dos switches de la capa de distribución.

5.2.3 Diseño de la topología de la capa núcleo

Refiera a la **Figura** del curso en línea

La capa núcleo de la LAN del estadio debe proporcionar conectividad de alta velocidad y alta disponibilidad. Tanto la red local como la red remota del estadio dependen de los switches del núcleo para la conectividad.

Requisitos de la capa núcleo

Algunos de los requisitos de diseño para la red de la capa núcleo son:

- Conectividad de alta velocidad hacia los switches de la capa de distribución
- Disponibilidad las 24 horas, todos los días
- Interconexiones direccionadas entre los dispositivos del núcleo
- Enlaces redundantes de alta velocidad entre los switches del núcleo y entre los dispositivos de la capa núcleo y de la capa de distribución

El diseño de la capa núcleo requiere conmutación de alta velocidad, de menor densidad y de varias capas. En el nuevo diseño, la red de la capa núcleo para el estadio puede implementarse sobre dos potentes switches de varias capas.

La capa núcleo está reservada para la conmutación del tráfico de alta velocidad; por lo tanto, en esta capa no se realiza el filtrado de paquetes, o se realiza en un nivel muy bajo.

En el entorno de una pequeña empresa, frecuentemente se combinan las capas de núcleo y de distribución. Esto puede denominarse núcleo colapsado o backbone colapsado.

Refiera a la **Figura** del curso en línea

Alta disponibilidad

La principal prioridad en la capa núcleo de la red es la alta disponibilidad. El diseñador de red necesita considerar todas las medidas que se puedan tomar para mejorar la confiabilidad y el tiempo de actividad.

Se deberían establecer los enlaces redundantes entre la capa núcleo y la capa de distribución. Siempre que sea posible, se debe implementar la instalación de componentes redundantes y tomar medidas adicionales para proporcionar aire acondicionado, alimentación y servicios redundantes a los dispositivos de la capa núcleo.

El uso de un protocolo de enrutamiento de Capa 3 como EIGRP u OSPF en la capa núcleo puede disminuir el tiempo que se demore en recuperarse de una falla del enlace. Las conexiones direccionadas entre los switches de la capa núcleo pueden proporcionar balanceo de carga de mismo costo así como también una rápida recuperación.

Velocidad

La siguiente prioridad en la capa núcleo es la velocidad. Casi todo el tráfico de red del estadio debe trasladarse a través de los dispositivos de la capa núcleo. Las interfaces de alta velocidad, la conectividad de fibra y las tecnologías como ***EtherChannel*** pueden proporcionar el suficiente ancho de banda como para admitir el nivel de tráfico y permitir que la red crezca en el futuro.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Trabajar con el estudio de caso de CompañíaCinematográfica para producir el diseño de red recomendado para la capa núcleo.

5.2.4 Creación del diseño lógico de red para la LAN

Creación del diagrama lógico de LAN

Refiera a la **Figura** del curso en línea

El paso final en el diseño de red LAN preliminar es crear el diagrama lógico de la nueva red del estadio. El diagrama muestra cómo se interconectan todas las distintas capas y dispositivos.

En la nueva LAN del estadio, cada uno de los 16 armarios de cableado contiene al menos un switch 2960. Debido a que hay tres módulos distintos en la red del estadio, se agregan seis switches a la capa de distribución que dirigen el tráfico entre la capa de acceso y la capa núcleo.

La capa núcleo está formada por dos switches de varias capas de nivel superior con redundancia. Se conectan a la capa de distribución y entre sí con enlaces gigabit.

El diseñador de red toma notas sobre el diagrama de red para indicar dónde se ubican los servidores y los servicios IP. Luego de completar el diseño de LAN cableado del campus, el diseñador planifica la porción de la red que admite la conectividad remota en la LAN del estadio.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un diagrama de la nueva LAN de CompañíaCinematográfica.

5.3 Diseño de WAN y soporte de trabajador remoto

5.3.1 Cómo determinar la conectividad para sitios remotos

Refiera a la **Figura** del curso en línea

En el margen empresarial, la red del estadio se conecta a Internet a través de DSL proporcionado por un ISP local. Los routers administrados por el ISP están en el estadio conectados al EdgeRouter de EstadioCompañía.

Extensión de servicios a ubicaciones remotas

Las dos ubicaciones remotas actuales, una oficina de venta de entradas ubicada en el centro y una tienda de recuerdos ubicada en un centro de compras local, utilizan el mismo proveedor ISP que el sitio principal del estadio. El ISP además les proporciona un servicio VPN administrado. Estas conexiones proporcionan a los sitios remotos acceso a las bases de datos que se encuentran en los servidores de las oficinas de administración del estadio.

Uno de los objetivos de alta prioridad de la nueva red del estadio es ampliar la red de video y voz a las ubicaciones remotas. Hay dos conexiones remotas adicionales planificadas:

- Una empresa de producción de películas, que se contrató para proporcionar video durante y después de los eventos, necesita conectarse a la red del estadio para intercambiar archivos.
- Un equipo deportivo que actualmente alquila espacio en el estadio se está expandiendo hacia una oficina remota. El equipo necesita acceder a los mismos recursos de red que utiliza en la LAN del estadio.

El ISP no admite QoS ni los SLA. El diseñador de red recomienda que el estadio instale una WAN aparte para proporcionar la QoS que se necesita para las aplicaciones de la empresa.

Refiera a la **Figura** del curso en línea

Cómo agregar nuevas conexiones WAN

El diseñador de red comprende que se requieren conexiones WAN dedicadas para cumplir con estos nuevos objetivos. Se envía un pedido de cotización a los proveedores de servicios de telecomunicaciones (***TSP***) de la zona para determinar el costo y la disponibilidad de los servicios WAN.

Debido a que el estadio se encuentra fuera de los límites de la ciudad, las opciones para la conectividad WAN se limitan a ***Punto a punto T1*** y ***Frame Relay***. Estos servicios están disponibles tanto para el estadio como para las ubicaciones remotas a través de un TSP local.

Aunque el servicio T1 punto a punto ofrece el mayor control sobre la calidad del servicio disponible para los sitios WAN, el servicio Frame Relay es menos costoso. El diseñador de red recomienda que el estadio utilice Frame Relay para conectarse a los sitios remotos hasta que en el área se encuentre disponible un servicio ***Metro Ethernet*** u otro servicio de alta velocidad.

Refiera a la **Figura** del curso en línea

Una ventaja de utilizar una conexión Frame Relay en lugar de las conexiones T1 punto a punto es que una sola conexión física al TSP puede proporcionar conectividad desde el estadio a varias ubicaciones remotas del sitio.

Tipos de conexión Frame Relay

Las redes Frame Relay transfieren datos utilizando uno de estos dos tipos de conexión:

- Circuitos virtuales conmutados (***SVC***): son conexiones temporales que se crean para cada transferencia de datos y que luego finalizan cuando se completa la transferencia de datos.
- Circuitos virtuales permanentes (***PVC***): son conexiones permanentes. Este tipo de conexión debe proporcionarse entre la red del estadio y los sitios WAN remotos.

Luego de discutirlo con la administración del estadio, el personal de CompañíadeRedes decide instalar una conexión Frame Relay desde el estadio hasta la tienda de recuerdos como instalación piloto para comprobar la conectividad WAN dedicada. Una ***instalación piloto*** es una pequeña implementación de una nueva tecnología de red que se utiliza para comprobar cómo la tecnología cumple con los objetivos de diseño.

5.3.2 Definición de los patrones de tráfico y el soporte de aplicación

Servicios de red para los sitios remotos

Refiera a la **Figura** del curso en línea

Cuando se determina el método físico para conectar los sitios remotos a la red principal del estadio, el diseñador de red debe además analizar de qué manera los trabajadores en los sitios remotos esperan utilizar los servicios de red. Los sitios remotos tienen algunas aplicaciones en común y algunos requisitos exclusivos. Algunos de los servicios que necesitan los sitios remotos son:

- Acceso a los servicios de e-commerce y de bases de datos
- Telefonía IP
- Monitoreo y vigilancia con video

Además, la nueva oficina remota del equipo requiere acceso al servidor de contabilidad y nómina de pagos del equipo que está ubicado en el estadio.

Los empleados de CompañíaCinematográfica necesitan poder monitorear las pantallas de video en forma remota en todo el estadio y transferir archivos de video a los servidores Web del estadio.

El diseñador realiza un cuadro con los flujos de tráfico desde cada conexión WAN a través de la red hacia las distintas ubicaciones del servicio. Este cuadro le proporciona al diseñador la información para crear normas para el firewall y los filtros ACL. Estas normas y filtros aseguran que los trabajadores de cada sitio remoto puedan acceder a los servicios que requieren.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Utilizando una red Frame Relay previamente configurada, examinar las conexiones a los dos sitios WAN.

5.3.3 Diseño de las opciones de conectividad terminal VPN

Respaldo del enlace Frame Relay

Refiera a la **Figura** del curso en línea

La oficina de venta de entradas y la tienda de recuerdos se conectan a la red del estadio utilizando las VPN de sitio a sitio a través de Internet. El ISP administra y es dueño de los routers del estadio y de los sitios remotos que proporcionan terminales para cada VPN. El diseñador de red planifica utilizar estas conexiones VPN como un respaldo para las conexiones dedicadas de Frame Relay en caso de que el enlace de este último falle. Además, el diseñador recomienda un enlace de respaldo desde cada uno de los dos nuevos sitios. Se planifica un segundo router extremo en el sitio principal para redundancia.

Respaldo para trabajadores remotos

La administración del estadio también desea respaldar a los trabajadores remotos quienes ocasionalmente trabajan desde sus hogares o desde otros sitios remotos. El personal del equipo deportivo, por ejemplo, necesita poder acceder al servidor del equipo en forma segura durante los viajes. El acceso VPN de cliente puede proveerse a través del mismo servicio administrado por el ISP. El diseñador recomienda a la administración del estadio investigar esta opción. Se ponen de acuerdo en contactar al ISP para hablar sobre la actualización.

5.3.4 Creación del diseño de red lógico para la WAN

Enrutamiento y direccionamiento IP

Refiera a la **Figura** del curso en línea

En la red existente, los sitios WAN utilizan sólo la VPN para conectarse al estadio. Las rutas estáticas simples son suficientes para asegurar la conectividad. El router de los servicios administrados por el ISP proporciona el direccionamiento DHCP a las LAN del sitio remoto.

Proporcionar conexiones WAN dedicadas y VPN a cada sitio requiere que el diseñador de red seleccione cuidadosamente los rangos de direcciones IP que se utilizan para cada sitio. Es posible que sea necesario cambiar los rangos de direcciones para los sitios remotos.

Al agregar la nueva conexión WAN a cada uno de los sitios se incrementa la cantidad de rutas posibles a la red del estadio de una a dos. Como consecuencia, el enrutamiento estático puede no ser el mejor método para asegurar conectividad a los servicios de la LAN del estadio. Es posible que sea necesario utilizar un protocolo de enrutamiento dinámico para permitir que las LAN remotas mantengan conectividad en el caso de una falla del enlace Frame Relay. El diseñador de red toma nota de esto para que se considere al diseñar la implementación del protocolo de enrutamiento del estadio.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Utilizando los routers preconfigurados para ejemplificar una conexión al sitio remoto en la red del estadio, observar lo que sucede al utilizar el enrutamiento estático y luego el enrutamiento dinámico.

5.4 Diseño de redes inalámbricas

5.4.1 Diseño de las opciones de cobertura y movilidad

Agregado de cobertura de red inalámbrica

Refiera a la **Figura** del curso en línea

Un objetivo principal del nuevo diseño es agregar cobertura de red inalámbrica a la red.

Como respuesta a las solicitudes de los medios locales, la administración del estadio agregó un punto de acceso inalámbrico económico para proporcionar Internet inalámbrica en la cabina de prensa. Algunos empleados además adquirieron routers para acceso inalámbrico proporcionando cobertura inalámbrica de baja calidad en las oficinas del equipo. Estos tipos de dispositivos no son lo suficientemente robustos como para una implementación de LAN inalámbrica a nivel empresarial.

Cobertura de la red inalámbrica

Para cumplir con los objetivos para el diseño de la nueva red del estadio, la cobertura inalámbrica es necesaria en cuatro áreas identificadas:

- La cabina de prensa
- Las áreas de relajación del equipo
- El restaurante del estadio
- Las suites de lujo ubicadas alrededor del estadio

Los dos puntos de acceso inalámbricos existentes deben cambiarse por dispositivos que sean más fáciles de administrar. Algunas áreas requieren de acceso inalámbrico para invitados. Las áreas del equipo además requieren de acceso seguro a los servidores de contabilidad y nómina de pagos del equipo.

La administración del estadio espera que la demanda de acceso inalámbrico crezca rápidamente. Prevén que se requerirá soporte para teléfono IP inalámbrico dentro de los próximos dos años. El soporte para teléfonos IP requiere de capacidades de roaming inalámbrico y mecanismos de QoS en la red inalámbrica.

Refiera a la **Figura** del curso en línea

Soluciones por cable e inalámbricas unificadas

La integración de la nueva red inalámbrica con la LAN por cable del estadio simplifica la administración y hace uso de la seguridad y redundancia de la infraestructura Ethernet.

Los puntos de acceso independientes conectados a los switches Ethernet en el armario de cableado pueden proporcionar la cobertura inalámbrica necesaria a las cuatro áreas previamente identificadas del estadio. El roaming inalámbrico limitado puede respaldarse creando VLAN inalámbricas que abarcan las áreas de cobertura inalámbrica y de red que se superponen.

Aunque esta solución cumple con los objetivos actuales de la red del estadio, el diseñador de red recomienda que el estadio compre puntos de acceso livianos ***LAP*** y ***Controladores de LAN inalámbrica*** para respaldar los requisitos inalámbricos. Los LAP no son dispositivos independientes; se basan en el controlador inalámbrico para la información de seguridad y para la configuración.

Las soluciones de red inalámbricas unificadas que incluyen el software del sistema de control inalámbrico ofrecen características avanzadas como la administración centralizada y muchos niveles de servicio para distintos tipos de clientes y usuarios. Estos sistemas permiten distintos niveles de QoS y seguridad para distintos tipos de uso inalámbrico.

Agregar el controlador inalámbrico y el software de administración a la red también simplifica la implementación de las características de roaming inalámbrico y de los teléfonos IP inalámbricos. Esta configuración elimina la necesidad de crear una única VLAN de extremo a extremo para el roaming inalámbrico.

Refiera a la **Figura** del curso en línea

La solución inalámbrica propuesta por el diseñador de red cumple con estos requisitos para la actualización de la red del estadio:

- **Escalabilidad**: los nuevos LAP pueden agregarse fácilmente y administrarse de manera centralizada.
- **Disponibilidad**: si algún AP falla, los AP pueden incrementar automáticamente la potencia de la señal.
- **Seguridad**: las políticas de seguridad que abarcan a toda la empresa se aplican a todas las capas de una red inalámbrica, desde la capa de radio pasando por la capa MAC y hasta la capa de red. Esta solución facilita la provisión de seguridad reforzada en forma uniforme, QoS y políticas del usuario. Estas políticas tratan las capacidades específicas de las distintas clases de dispositivos, como los escáneres portátiles, los PDA y las computadoras portátiles. Las políticas de seguridad además proporcionan descubrimiento y mitigación de ataques DoS y detección y rechazo de AP maliciosos. Estas funciones se producen en toda la WLAN administrada.
- **Facilidad de administración**: la solución proporciona administración de radiofrecuencia dinámica en todo el sistema, que incluye características que ayudan al funcionamiento ininterrumpido de las operaciones inalámbricas, como la ***asignación dinámica de canales***, el ***control de energía de transmisión*** y el balanceo de carga. La interfaz gráfica única para las políticas que abarcan toda la empresa incluye las VLAN, la seguridad y la QoS.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de pantalla completa

5.4.2 Ubicación de los AP inalámbricos

Refiera a la **Figura** del curso en línea

Los resultados del relevamiento del sitio inalámbrico del estadio indican que el restaurante requiere al menos dos AP para proporcionar una cobertura inalámbrica de alta calidad.

El diseñador de red determina que para contener la señal inalámbrica dentro del restaurante es mejor instalar los AP direccionales contra las dos paredes externas.

El relevamiento del sitio no reveló ningún problema que pueda ocasionar una interferencia inalámbrica dentro de la zona del restaurante. Sin embargo, el horno de microondas de la zona de la cocina puede ocasionar interferencias cerca de la barra. Según los AP seleccionados, es posible que sea necesario realizar un segundo relevamiento para asegurar que la cobertura sea adecuada.

Cada uno de los 20 conjuntos de aplicaciones de lujo ubicados alrededor del estadio requiere de un único AP de baja potencia colocado en el cielorraso al centro de la habitación.

La cabina de prensa actualmente tiene un único AP independiente que no posee la cobertura adecuada. Se recomiendan dos nuevos AP livianos.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizando el plano del edificio de las oficinas de CompañíaCinematográfica y con los resultados del relevamiento inalámbrico indicado, seleccionar las antenas y los AP correctos para la instalación.

5.4.3 Redundancia y capacidad de recuperación en una red inalámbrica

Consideraciones de disponibilidad

Refiera a la **Figura** del curso en línea

La disponibilidad de una conexión inalámbrica depende de los siguientes factores:

- La ubicación del AP
- La potencia de la señal del AP
- La cantidad de usuarios que comparten la conectividad del AP

Las redes inalámbricas que utilizan AP independientes usualmente tienen los AP configurados e implementados con el canal y la potencia establecidos en forma estática. El diseñador de red determina las configuraciones de potencia y canal. Una vez configurados, estos parámetros no toman en cuenta la variabilidad de las señales inalámbricas a través del aire. Los relevamientos del sitio registran la cobertura en momentos específicos. Es difícil para el diseñador anticipar la reconfiguración de oficinas y la introducción de nuevas fuentes de interferencia.

Reconfiguración dinámica

A diferencia de los AP autónomos, los controladores LAN inalámbricos automáticamente determinan la potencia de la señal entre los AP livianos dentro de la misma red. Estos controladores pueden utilizar esta información para crear una topología de radiofrecuencia dinámica óptima para la red.

Cuando un LAP de Cisco arranca, inmediatamente busca un controlador LAN inalámbrico dentro de la red. Cuando detecta un controlador LAN inalámbrico, el AP envía mensajes de vecino encriptados que incluyen la dirección MAC y la potencia de la señal de cualquier AP vecino. En una red con un solo controlador LAN inalámbrico, el controlador sintoniza cada canal AP para obtener la mejor potencia de señal, cobertura y capacidad.

Refiera a la **Figura** del curso en línea

Usuarios de la centralización del balanceo de carga

A través de mensajes encriptados enviados por aire, los controladores LAN inalámbricos de Cisco detectan toda la red. Estos controladores además detectan la potencia de la señal entre los AP. Cuando un cliente busca un AP para conectarse, se envía una sonda al controlador desde cada AP que escucha la solicitud del cliente. El controlador determina qué AP responde a la solicitud del cliente tomando en cuenta la potencia de la señal del cliente y la relación señal a ruido.

Por ejemplo, un AP adyacente puede proporcionar un servicio equivalente pero con una menor potencia de señal. El controlador determina qué AP debe responder a la sonda del cliente en función de la potencia de su señal, o indicador de potencia de la señal del receptor (***RSSI***).

Estas medidas mejoran la disponibilidad de los servicios inalámbricos dentro de la WLAN. Los controladores inalámbricos ubicados de manera centralizada en el centro de datos se benefician con las conexiones redundantes y de alta disponibilidad que se incluyen en la LAN por cable.

5.4.4 Creación del diseño de red lógico para la WLAN

Direccionamiento IP en una WLAN

Refiera a la **Figura** del curso en línea

El diseñador de red también debe considerar la estructura del direccionamiento IP cuando planifique el roaming inalámbrico en una WLAN. En el caso de los AP independientes, se crea una única VLAN y se amplía a todos los armarios de cableado para conectar los AP en la misma red IP de Capa 3. Sin embargo, si una gran cantidad de usuarios inalámbricos se conectan a la red, los broadcast se convierten en un problema. La red ya no es escalable.

Roaming de Capa 3

Cuando se utilizan controladores inalámbricos y AP livianos se puede introducir el roaming de Capa 3 en una red. No es necesario ampliar las VLAN a todos los AP de la red para mantener una subred inalámbrica plana.

Con el controlador inalámbrico, los AP livianos se instalan en la infraestructura de la subred normal y se les otorga una dirección IP local para la subred a la cual se implementan. Todo el tráfico proveniente de clientes inalámbricos se coloca en un paquete que se canaliza a través de la red subyacente hacia el controlador LAN inalámbrico.

Los dispositivos del cliente reciben sus direcciones IP del controlador, no de la subred del área del edificio en donde residen. La infraestructura IP subyacente permanece oculta ante el cliente. El controlador administra todo el roaming y tunneling para que los clientes puedan mantener la misma dirección IP a medida que itineran.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad

Dado un diagrama de red que incluye un controlador inalámbrico y un AP, responder las preguntas sobre el direccionamiento IP.

5.5 Incorporación de seguridad

5.5.1 Colocación de artefactos y funciones de seguridad

Refiera a la **Figura** del curso en línea

Las amenazas a las redes pueden tomar muchas formas diferentes, tanto de fuentes internas como externas. La simple colocación de un firewall en el margen empresarial no garantiza la seguridad de la red. El diseñador de red debe identificar qué datos y comunicaciones están en riesgo y cuáles son los posibles orígenes de los ataques. Los servicios de seguridad necesitan entonces colocarse en los puntos correspondientes en todo el diseño de la red para evitar los posibles ataques.

Los servidores de e-commerce de la red del estadio contienen información del cliente que pueden incluir detalles bancarios y de tarjeta de crédito. Los usuarios acceden a estos servidores desde la red del estadio y a través de Internet.

Los servidores administrativos del equipo y de administración del estadio contienen información de la nómina de pagos y del personal. Estos servidores, y la infraestructura que transporta los datos que ellos contienen, deben estar correctamente asegurados para proteger esta información del uso no autorizado.

También se deben considerar las medidas de seguridad relacionadas con la red inalámbrica del estadio.

Refiera a la **Figura** del curso en línea

Los servicios de seguridad ayudan a proteger los dispositivos y la red ante intrusiones, manipulaciones, alteración de datos e interrupción de servicios a través de los ataques de denegación de servicio (***DoS***). Las categorías primarias de los servicios de seguridad incluyen:

- La protección de la infraestructura
- La conectividad segura
- La detección, defensa y mitigación de amenazas

La protección de la infraestructura

La seguridad de la red comienza con la seguridad de los mismos dispositivos de red. Esto involucra asegurar los routers basados en el software IOS de Cisco, los switches y los appliances contra ataques directos e indirectos. Esta protección ayuda a asegurar la disponibilidad de la red para el traslado de datos.

La conectividad segura

Es esencial para evitar que los usuarios no autorizados accedan a la red. Esto puede realizarse garantizando que la red física es segura y solicitando autenticación para obtener acceso a los servicios inalámbricos. Los empleados del estadio y los invitados deben estar asignados a distintos SSID y WLAN. Asegurar los datos mientras están en tránsito puede hacerse utilizando las VPN o la encriptación de datos.

La detección de amenazas, la defensa y la mitigación

Los firewall, IDS, IPS y las ACL proporcionan protección contra amenazas y atacantes. Las ACL y las normas de firewall filtran el tráfico para permitir sólo el tráfico deseable a través de la red.

Refiera a la **Figura** del curso en línea

Implementación de servicios de seguridad

Los servicios de seguridad no son efectivos si no se implementan en las ubicaciones correctas en toda la red. Los firewall y los filtros colocados en el margen empresarial no protegen los servidores ante los ataques desde el interior de la LAN. El diseñador de red analiza los diagramas del flujo de tráfico que se crearon anteriormente y que muestran:

- Los recursos a los que acceden los usuarios internos
- Los recursos a los que acceden los usuarios externos
- Las rutas que este acceso toma a través de la red

Esta información ayuda al diseñador a colocar los servicios de seguridad en los lugares correspondientes para hacer cumplir las políticas de seguridad del estadio.

Uso de servicios integrados

Siempre que sea posible, el diseñador de red utiliza servicios integrados como las características de firewall basadas en el IOS y módulos IDS para eliminar la necesidad de contar con dispositivos de seguridad adicionales. En una red más grande, es necesario utilizar dispositivos separados debido a que el procesamiento adicional puede sobrecargar los routers y switches.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Determinar el lugar correspondiente para proporcionar el servicio de seguridad.

5.5.2 Implementación de filtrado y listas de control de acceso

Refiera a la **Figura** del curso en línea

El diseñador de red trabaja con el personal de TI del estadio para definir el ***conjunto de reglas del firewall*** que se implementará en la actualización de red del estadio.

Algunos ejemplos del conjunto de reglas del firewall incluyen estas afirmaciones:

- **Denegar todo tráfico entrante cuyas direcciones de red coincidan con las direcciones IP internas registradas**: el tráfico entrante no debería originarse de direcciones de red que coincidan con direcciones internas.
- **Denegar todo tráfico entrante a las direcciones externas del servidor**: esta regla incluye denegar las direcciones traducidas del servidor, a excepción de los puertos permitidos.
- **Denegar todo tráfico entrante con solicitud de eco ICMP**: esta regla evita que los hosts de la red interna reciban solicitudes de ping que se generan fuera de la red confiable.
- **Denegar todo broadcast local de dominio Microsoft entrante, Active Directory y puertos del servidor SQL**: el tráfico de dominio Microsoft debe trasladarse a través de las conexiones VPN.
- **Permitir DNS (UDP 53) al servidor DNS**: permitir búsquedas DNS externas.
- **Permitir el tráfico Web (TCP 80/443) desde cualquier dirección externa hacia el rango de direcciones del servidor Web.**
- **Permitir tráfico (TCP 21) hacia los rangos de dirección del servidor FTP**: si se proporcionan servicios FTP a usuarios externos, esta regla permite el acceso al servidor FTP. Como recordatorio, cuando se utilizan los servicios FTP, la información de cuenta de usuario y contraseña se transmite en texto sin cifrar. El uso de FTP pasivo (PASV) negocia un puerto de datos al azar en lugar del uso del puerto 20 TCP.
- **Permitir tráfico (TCP 25) hacia el servidor SMTP**: permite a los servidores y usuarios SMTP externos acceder al servidor de correo SMTP interno.
- **Permitir tráfico (TCP 143) hacia el servidor IMAP interno**: permite a los clientes IMAP externos acceder al servidor IMAP interno.

Refiera a la **Figura** del curso en línea

Las políticas de seguridad de la administración del estadio determinan los permisos del grupo y del usuario para los recursos. El diseñador además cumple con las prácticas recomendadas definidas por los fabricantes de sistemas operativos de servidor. Estas prácticas ayudan a identificar y a filtrar el tráfico que se sabe que es malicioso.

Cuando se diseñan conjuntos de reglas del firewall y las ACL, la política general es denegar todo el tráfico que no esté específicamente autorizado o que no se origina en respuesta a una investigación permitida.

Conjuntos de reglas y listas de control de acceso

Los conjuntos de reglas del firewall se usan para crear las afirmaciones de la ACL que se implementan en los routers y en los artefactos del firewall. Cada conjunto de reglas del firewall requiere más de una afirmación de la ACL y puede requerir tanto una ubicación interna como una externa.

5.5.3 Actualización de la documentación de diseño de la red lógica

Refiera a la **Figura** del curso en línea

La documentación del diseño incluye todos los conjuntos de reglas del firewall y las ACL y define dónde se implementan. Las afirmaciones del conjunto de reglas pasan a formar parte de la documentación de la política de seguridad de la administración del estadio.

La documentación de los conjuntos de reglas del firewall y la ubicación de la ACL ofrecen estos beneficios:

- Proporciona evidencia de que la política de seguridad se implementa en la red
- Asegura que cuando los cambios sean necesarios, se conozcan y evalúen todas las instancias de un permiso o rechazo
- Ayuda con la resolución de problemas mediante el acceso a aplicaciones o segmentos de la red

Refiera a la actividad de “**Packet Tracer**” del curso en línea

Actividad de Packet Tracer

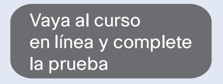
Utilizando el diagrama del margen empresarial de la red del estadio, implementar las ACL para que coincidan con un conjunto de reglas definidas.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Dada una política de seguridad para la empresa CompañíaCinematográfica, crear un conjunto de reglas del firewall e implementar las ACL para aplicar el conjunto de reglas.

Resumen del capítulo



Examen del capítulo

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 6

Uso del direccionamiento IP en el diseño de red

Introducción

Refiera a la **Figura** del curso en línea

6.1 Creación de un diseño de direccionamiento IP apropiado

6.1.1 Uso de esquemas de direccionamiento y enrutamiento jerárquico

Esquema de direccionamiento IP

Refiera a la **Figura** del curso en línea

En el esquema de direccionamiento IP existente para la red del estadio, el administrador de red seleccionó la dirección de red IP privada 192.168.2.0/23. Se utilizaron otras dos subredes, 192.168.4.0/24 y 192.168.5.0/24, para direccionar las dos ubicaciones remotas. El administrador asignó direcciones IP únicas de cliente, mediante DHCP y direcciones estáticas, a cada uno de los distintos dispositivos de red.

El esquema de direccionamiento actual que se utiliza en el estadio no es adecuado porque no puede respaldar la ampliación planificada de la red. Además, los dos AP inalámbricos asignan direcciones IP que se superponen con las direcciones de EstadioCompañía existentes.

El nuevo diseño necesita utilizar un esquema de direccionamiento IP que asegure que cada dispositivo de red tenga asignado una única dirección IP.

Refiera a la **Figura** del curso en línea

Si se asigna la misma dirección IP a más de un dispositivo en una red, se produce un conflicto de IP. Un conflicto de IP en la red significa que los paquetes no se entregan de manera confiable a los dispositivos con la misma dirección IP.

Con una correcta planificación de red, un nuevo esquema de direccionamiento IP puede admitir el enrutamiento jerárquico y proporcionar una estructura de Capa 3 eficiente. La asignación de direcciones IP debe planificarse y documentarse para:

- Prevenir la duplicación de direcciones
- Proporcionar y controlar el acceso
- Monitorear la seguridad y el desempeño
- Admitir un diseño modular
- Admitir una solución escalable que utilice agregación de rutas

Mediante un diseño de direccionamiento IP jerárquico, la red del estadio es más fácil de respaldar.

Refiera a la **Figura** del curso en línea

Uso de un esquema de direccionamiento IP jerárquico

Un esquema de direccionamiento IP plano no cumple con los requisitos de escalabilidad de la red del estadio.

Una red con la correcta asignación e implementación de los bloques de direcciones IP tiene las siguientes características:

- Estabilidad de enrutamiento
- Disponibilidad del servicio
- Escalabilidad de la red
- ***Modularidad de la red***

El uso de un esquema de direccionamiento IP jerárquico para la red del estadio facilita el incremento del tamaño de la red. Una red más grande puede admitir más usuarios, puestos de venta de entradas, oficinas remotas y tiendas de recuerdos.

Un esquema de direccionamiento IP jerárquico correctamente diseñado facilita además la realización de la ***sumarización de ruta***.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Diseñar y asignar una dirección a una topología.

6.1.2 Sumarización y subredes con clase

Refiera a la **Figura** del curso en línea

Para admitir la sumarización se debe diseñar una red que tenga subredes contiguas. Si una red es contigua, todas las subredes de la red son adyacentes a todas las otras subredes de la misma red.

Una ***red no contigua*** tiene subredes no adyacentes o subredes que están separadas de otras subredes de la misma red por medio de otras redes.

El direccionamiento IP mal planificado puede dar como resultado una red no contigua. Las redes no contiguas pueden ocasionar problemas de enrutamiento porque hay más de una entrada de resumen de rutas en la tabla de enrutamiento que se utiliza para alcanzar las subredes de una red. Los protocolos de enrutamiento pueden no enrutar correctamente el tráfico a menos que se los configure en forma manual debido a que algunos protocolos de enrutamiento resumen las rutas de manera automática y predeterminada.

Inhabilitación de la sumarización automática

Generalmente, se aconseja la sumarización automática. Sin embargo, en el caso de subredes no contiguas, se debe ingresar el siguiente comando para el Routing Information Protocol versión 2 (***RIPv2***) y para EIGRP para así inhabilitar la sumarización automática:

```
Router(config-router)#no auto-summary
```

Actividad de Packet Tracer

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Resolver los problemas de una red no contigua.

6.1.3 Uso de VLSM para el diseño del direccionamiento IP

Refiera a la **Figura** del curso en línea

La administración del estadio y el diseñador de red creen que la red del estadio crecerá en forma considerable durante los próximos dos años. Para cumplir con el requisito de escalabilidad, el diseñador propone utilizar un esquema de direccionamiento IP jerárquico y un protocolo de enrutamiento sin clase.

Máscara de subred de longitud variable (*VLSM*)

El diseñador de red utiliza la VLSM para crear el esquema de subred para la red propuesta. El uso de la VLSM elimina el requisito que dice que todas las subredes de la misma red principal deben

tener la misma cantidad de direcciones de host y la misma duración de prefijo. La VLSM admite un uso más eficiente del espacio de direcciones IP. La VLSM además habilita los routers para que resuman rutas en los límites diferentes de los límites con clase.

Enrutamiento entre dominios sin clase (*CIDR*)

Cuando la VLSM se utiliza en el esquema de direccionamiento IP, el diseñador debe utilizar un protocolo de enrutamiento que admita el CIDR.

Los protocolos de enrutamiento con clase no envían la información de la máscara de subred o de duración de prefijo con las actualizaciones de enrutamiento. Estos protocolos dependen de las máscaras de subred predeterminada para definir la porción de red de las direcciones IP.

Los protocolos de enrutamiento sin clase envían la información de la duración de prefijo junto con la ruta en las actualizaciones del enrutamiento. Estos protocolos habilitan los routers para que determinen la porción de red de la dirección sin utilizar las máscaras predeterminadas.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Aplicar la VLSM a un esquema de enrutamiento jerárquico.

6.1.4 Uso de la sumarización y el enrutamiento CIDR

CIDR y sumarización

Refiera a la **Figura** del curso en línea

El diseño jerárquico de la red del estadio pretende facilitar la sumarización de ruta y reducir el procesamiento del protocolo de enrutamiento. La sumarización de ruta también se conoce como agregación de ruta. Es el proceso de publicar un grupo de direcciones contiguas como una única entrada con un prefijo o con una máscara de subred más corta y menos específica.

Debido a que el CIDR ignora los límites de los bordes con clase, habilita la sumarización con las VLSM que son más cortas que la máscara con clase predeterminada. Una dirección de red cuya duración de prefijo sea más corta que la duración de prefijo con clase predeterminada se conoce como ***superred***. Un ejemplo de una dirección de superred es 172.16.0.0/14. El prefijo predeterminado para la dirección 172.16.0.0 de Clase B es 16 bits. Mediante un prefijo /14 se pueden resumir cuatro direcciones de Clase B contiguas en una entrada en la tabla de enrutamiento.

Este tipo de sumarización ayuda a reducir la cantidad de entradas en las actualizaciones de enrutamiento y disminuye la cantidad de entradas en las tablas de enrutamiento locales. El resultado es una búsqueda más rápida de la tabla de enrutamiento.

Refiera a la **Figura** del curso en línea

Sumarización y direcciones de prefijo

Los protocolos de enrutamiento sin clase incluyen la duración de prefijo y la máscara de subred en la dirección de 32 bits de las actualizaciones de enrutamiento.

Una jerarquía compleja de redes y subredes de tamaños variables puede resumirse en varios puntos mediante una ***prefijo de dirección***. Por ejemplo, una ruta de resumen puede incluir un prefijo de 14 bits que es común a todas las direcciones a las que se puede llegar a través de un router. El prefijo:

172.16.0.0/14 o

10101100.00010000.00000000.00000000

con una máscara de subred de:

11111111.11111100.00000000.00000000

resume las subredes 172.16.0.0 /16, 172.17.0.0 /16, 172.18.0.0 /16 y 172.19.0.0 /16 en una dirección total.

La sumarización de ruta reduce la carga a los routers ascendentes.

Para que la sumarización funcione correctamente, se deben asignar cuidadosamente las direcciones en forma jerárquica para que las direcciones resumidas compartan los mismos bits de orden superior.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Utilizar la notación del CIDR para asegurar la sumarización de ruta dentro de una topología que utilice OSPF o EIGRP.

6.2 Creación de la dirección IP y del esquema de denominación

6.2.1 Diseño del esquema de dirección IP de la LAN lógica

Refiera a la **Figura** del curso en línea

Para el diseñador de red, algunas decisiones sobre la asignación de direcciones IP para la red del estadio son simples. Por ejemplo, el uso de un rango de dirección privada para la LAN en lugar de un rango de dirección pública. Otras decisiones requieren de una planificación más cuidada.

Cuando se crea un esquema de asignación de direcciones IP, el diseñador sigue estos pasos:

Paso 1: Planifica todo el esquema de asignación de direcciones antes de asignarlas.

Paso 2: Permite un crecimiento importante.

Paso 3: Comienza con las direcciones de resumen de la red de núcleo y continúa hacia el extremo.

Paso 4: Identifica qué máquinas y dispositivos requieren direcciones asignadas en forma estática.

Paso 5: Determina dónde y cómo se implementa la asignación de direcciones dinámicas.

Estas consideraciones se aplican si el diseñador está usando o no la asignación de direcciones públicas o privadas.

Refiera a la **Figura** del curso en línea

Varios criterios determinan el diseño de la dirección de red:

- La cantidad de hosts y dispositivos de red que actualmente admite la red
- Cuánto crecimiento se anticipa
- La cantidad de hosts que deben poder alcanzarse desde las redes que no son parte de la LAN local o Intranet
- La disposición física de la red
- Las políticas de seguridad y enrutamiento implementadas

No hay muchos hosts en la red actual del estadio. Aproximadamente hay 500 hosts conectados a la red cableada y una pequeña cantidad de hosts se conectan en forma inalámbrica. Según el crecimiento previsto de EstadioCompañía, el diseñador de red calcula al menos 2000 dispositivos de usuario final dentro de dos años. Esta cantidad incluye impresoras, escáneres, AP, dispositivos inalámbricos, teléfonos IP y cámaras en la red que necesitan direcciones IP individuales. Para dar lugar a este crecimiento, el diseñador decide utilizar un bloque privado de direcciones IP de Clase B.

Refiera a la **Figura** del curso en línea

Posibilidad de conexión de los hosts

Algunos hosts de la red deben poder conectarse desde redes que no forman parte de la LAN local o Intranet. Para ser accesibles desde Internet, los servidores y servicios deben tener asignada una dirección IP con registro público. Es necesario que haya suficientes direcciones públicas para utilizar con la NAT. En el estadio, los dos servidores del equipo y los servidores de e-commerce y

Web ofrecen servicios a los que se debe poder acceder desde Internet. El diseñador de red concluye que son apropiados los bloques de subred /27 existentes de las 30 direcciones públicas del proveedor de servicios de Internet.

Distribución física de la red

En el estadio se encuentran disponibles 16 armarios de cableado individuales para respaldar la distribución geográfica de los dispositivos de usuario final. Una buena política es restringir las subredes IP a las ubicaciones individuales físicas de los armarios de cableado. Se necesitan direcciones de red separadas para cada conexión redundante entre los routers, switches de Capa 3 y la WAN.

Políticas de enrutamiento y seguridad

Algunas veces se necesitan redes IP adicionales para separar el tráfico para fines de seguridad o filtrado. En estos casos usualmente se crean subredes IP separadas. Los teléfonos IP e inalámbricos requieren redes IP separadas.

La elección de un protocolo de enrutamiento afecta la manera en que se asignan las direcciones en una red. Algunos protocolos de enrutamiento no admiten la asignación de direcciones IP sin clase. También se debe considerar la sumarización predeterminada que se implemente en el protocolo de enrutamiento. El diseñador observa que el esquema de asignación de direcciones de Clase B planificado requiere un protocolo de enrutamiento sin clase.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Determinar una estrategia apropiada para la asignación de direcciones IP para la red de CompañíaCinematográfica.

6.2.2 Determinación de los bloques de asignación de direcciones

Refiera a la **Figura** del curso en línea

El diseñador de red determina la cantidad de redes IP o subredes que se requieren sobre la base de la estrategia de asignación de direcciones IP utilizada para el estadio.

El diseñador cuenta la cantidad de subredes y observa la cantidad actual y proyectada de usuarios o dispositivos en cada red.

Cada armario de cableado tiene un mínimo de cuatro subredes:

- Datos
- Voz IP
- Vigilancia con video y video de los encuentros deportivos
- Servicios de administración de red

En algunas áreas son necesarias más de cuatro subredes para separar el tráfico. En los switches se utilizan las VLAN para respaldar cada subred separada.

El diseñador registra la siguiente información para cada ubicación dentro de la red:

- Ubicación y descripción
- Tipo de red o VLAN
- Cantidad de redes y hosts

Ubicación y descripción

El diseñador identifica cada ubicación documentando el armario de cableado o el número de sala del centro de datos y una descripción del área del estadio con la cual se conecta el armario de cableado.

Tipo de red o VLAN

La documentación del tipo de VLAN o red habilita al diseñador a estimar en forma precisa el probable crecimiento de la cantidad de hosts. Una VLAN de datos puede aumentar su tamaño más que una VLAN que respalda teléfonos IP. Una red punto a punto de Capa 3 usualmente no se amplía fuera de las dos direcciones host originales.

Cantidad de redes y de hosts por red

A continuación, el diseñador cuenta y enumera la cantidad de redes y la cantidad de hosts por red que existen en el nuevo diseño. Este conteo representa los requisitos de dirección actuales. El diseñador puede entonces calcular el crecimiento en cada área para determinar el tamaño de la red o subred IP.

Los requisitos de la red inalámbrica se especifican en forma separada. Agregar dispositivos que se conectan en forma inalámbrica aumenta la cantidad de direcciones IP que se necesitan sin sumar switches ni puertos nuevos.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Determinar la cantidad de redes y de hosts en una sección de la red de CompañíaCinematográfica.

6.2.3 Diseño de la estrategia de enrutamiento

El diseñador de red necesita seleccionar un protocolo de enrutamiento que cumpla con estos requisitos del estadio:

- Funcionamiento del enrutamiento sin clase que admite VLSM
- Pocas e infrecuentes actualizaciones de la tabla de enrutamiento para reducir el tráfico
- Rápida convergencia en el caso de una falla

Refiera a la **Figura** del curso en línea

El estadio tiene la restricción de que el personal de creación de redes actual debe ser capaz de solucionar problemas de la red resultante. Por lo tanto, debe ser fácil resolver problemas del protocolo de enrutamiento y reconfigurar en caso de fallas.

Dos miembros del personal de red tienen experiencia en el uso de EIGRP. Debido a que EIGRP cumple con todos los requisitos del estadio, el diseñador de red selecciona EIGRP en lugar de OSPF y RIPv2.

EIGRP es un protocolo de enrutamiento patentado por Cisco. Todos los dispositivos del estadio que participan en el enrutamiento dinámico deben ser dispositivos de Cisco.

Balanceo de carga EIGRP

Refiera a la **Figura** del curso en línea

En el diseño de la red del estadio son necesarios los enlaces redundantes y de respaldo para cumplir con los requisitos de disponibilidad. EIGRP es una buena opción ya que puede admitir el balanceo de carga sobre estos enlaces adicionales. De manera predeterminada, EIGRP instala hasta cuatro rutas de igual costo hacia el mismo destino de la tabla de enrutamiento. Para controlar la cantidad de rutas que instala EIGRP, se utiliza el comando **`maximum-paths`**. Los valores aceptables para el comando **`maximum-paths`** están entre 1 y 6. Si se configura un valor de 1, se deshabilita el balanceo de carga ya que sólo se puede instalar 1 ruta en la tabla de enrutamiento para un destino específico.

Balanceo de carga con distinto costo

Hay veces, como durante la venta de entradas para eventos populares, que puede ser necesario utilizar enlaces de respaldo para balancear la carga de tráfico pesado. Debido a que los enlaces de

respaldo no siempre tienen el mismo costo de enrutamiento que los enlaces principales, no se balancea la carga del tráfico en los enlaces de respaldo de manera predeterminada. Se puede configurar un router en una red EIGRP para que utilice el balanceo de carga con distinto costo mediante el comando **variance**.

Una variación (variance) es un valor que utiliza EIGRP para determinar si instala o no una ruta específica en la tabla de la ruta para que esté disponible para el balanceo de carga. La fórmula que EIGRP utiliza para establecer el rango de costos aceptables de la ruta es igual a *variance por métrica*. Utilice el comando **variance** seguido por un valor entre 1 y 128. Un ejemplo del comando es:

```
Router(config-router)# variance 2
```

Dividir el tráfico de esta forma evita que un único camino se sobrecargue con tráfico pesado cuando hay caminos alternativos disponibles.

Refiera a la **Figura** del curso en línea

Autenticación

En la red del estadio hay fabricantes y sitios remotos que participan del enrutamiento de la red. Es importante saber que las actualizaciones de enrutamiento provienen de routers confiables. Los protocolos de enrutamiento pueden configurarse para aceptar solamente las actualizaciones provenientes de dispositivos confiables mediante la autenticación de vecino. Cuando en un router se configura la autenticación de vecino, el router autentica el origen de cada paquete de actualización de enrutamiento que recibe.

Hay dos tipos de autenticación de vecino: la autenticación de texto sin cifrar y la autenticación de algoritmo Message Digest versión 5 (***MD5***). El uso de la autenticación MD5 es una práctica de seguridad recomendada porque la clave o contraseña no puede interceptarse y leerse en tránsito.

Administración de clave

En la autenticación MD5, cada router vecino participante se configura para que comparta una clave de autenticación. Los protocolos de enrutamiento RIPv2 y EIGRP ofrecen la función adicional de administrar las claves mediante cadenas de claves. Se puede configurar una serie de claves y el software IOS de Cisco pasa por cada una de éstas. Esto disminuye la posibilidad de comprometer las claves.

Toda definición de clave debe especificar el intervalo de tiempo durante el cual la clave está activa (su "vida útil"). Luego, durante una cierta vida útil de la clave, se envían los paquetes de actualización de enrutamiento con la clave activada. Se recomienda que para un cierto grupo de claves, los tiempos de activación de la clave se superpongan para evitar que se produzcan períodos de tiempo durante los cuales no haya clave activa. Si se produce un período de tiempo durante el cual no haya una clave activa, no se podrá realizar la autenticación de vecino y por lo tanto fallarán las actualizaciones de enrutamiento.

Para establecer el período de tiempo durante el cual es válido enviar una clave de autenticación con una cadena de claves, utilice el comando **send-lifetime**. El comando **accept-lifetime** establece el tiempo durante el cual el router aceptará las actualizaciones con la clave. El valor predeterminado para ambos comandos es infinito.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Configurar una red EIGRP con varios routers.

6.2.4 Planifique la sumarización y la distribución de rutas

Refiera a la **Figura** del curso en línea

En un diseño jerárquico, la sumarización de ruta se produce en los dispositivos de Capa 3 que actúan como gateways para muchas redes IP contiguas. Estas rutas resumidas luego se publican

hacia la capa núcleo de la red. La sumarización en la LAN del estadio se produce en los routers de la capa de distribución y en los switches de Capa 3.

EIGRP habilita la sumarización sin clase con máscaras que son diferentes de la máscara con clase predeterminada. Este tipo de resumen ayuda a reducir el número de entradas en las actualizaciones de enrutamiento y disminuye la cantidad de entradas en las tablas de enrutamiento locales. La sumarización reduce la cantidad de ancho de banda utilizado por las actualizaciones de enrutamiento, lo cual da como resultado búsquedas más rápidas en la tabla de enrutamiento.

EIGRP incluye una característica de sumarización de ruta automática. Sin embargo, esta sumarización automática se produce sólo en el límite predeterminado de la red con clase. Esta característica no es apropiada para el diseño de red del estadio. Para poder resumir las subredes del esquema de asignación de direcciones de Clase B propuesto se debe inhabilitar la sumarización de ruta automática en EIGRP.

Refiera a la **Figura** del curso en línea

Cuando se inhabilita la sumarización automática, se debe configurar la sumarización manual.

El diseñador de red determina un resumen de rutas mediante estos pasos:

Paso 1: Convierta las direcciones de las redes a formato binario.

Paso 2: Encuentre la máscara de subred que se debe utilizar para el resumen de rutas.

Paso 3: Determine la dirección de red del resumen de rutas.

Cuando se utilizan resúmenes de rutas, el diseñador debe asegurar que las rutas no se superpongan con otras rutas resumidas o individuales.

Cuando se determina la ruta, el diseñador configura esta información en el router en forma manual.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Hacer coincidir los resúmenes de rutas con las redes que publican.

6.2.5 Diseño del esquema para asignación de direcciones

Bloques de direcciones IP

Refiera a la **Figura** del curso en línea

Sobre la base de la información que se incluye en los cuadros de los Requisitos de la red IP, el diseñador de red determina el tamaño de los bloques de direcciones IP que se necesitan para cada área de la red. El diseñador agrupa las áreas que tienen requisitos similares para reducir el número de máscaras de subred diferentes que deben admitirse.

Si todos los dispositivos necesitaran direcciones IP públicas registradas, la agrupación sería en vano. Sin embargo, cuando se utilizan direcciones IP privadas, es aconsejable agrupar las áreas. Al reducir el número de combinaciones de subred, el diseñador simplifica las configuraciones. Esto facilita la tarea de respaldo y resolución de problemas del personal de la red actual del estadio. El diseñador decide admitir 4 máscaras de subred: /19, /22, /24 y /30.

Asignación de bloques de direcciones

El diseñador cumple con un proceso paso a paso para asignar las subredes. Comienza con el bloque más grande y continúa hasta el más pequeño.

El diseñador de red reserva la subred 0 y la subred que contiene la dirección con sólo números 1 para un caso especial. En ciertas situaciones de red más complejas, estas subredes pueden requerir una configuración única. Aunque la red del estadio no tiene en este momento ninguna condición que pueda ocasionar que estas redes se desestabilicen, el diseñador no puede predecir qué situaciones podrían presentarse. El esquema de red IP que el diseñador utiliza tiene una cantidad suficiente de direcciones utilizables; por lo tanto, no es necesario emplear estas subredes.

Refiera a la **Figura** del curso en línea

Uso de la subred 0 y de la subred con sólo números 1

Aunque no sea una práctica recomendada, el uso de la subred 0 y de la subred con sólo números 1 está explícitamente permitido a partir de la versión 12.0 del software IOS de Cisco. En las versiones anteriores, la subred 0 podía utilizarse ingresando el comando de configuración global **`ip subnet-zero`**.

El documento RFC 1878 establece que la práctica de excluir las subredes con solo números 0 y las subredes con sólo números 1 es obsoleta. El software moderno es capaz de utilizar todas las redes definibles.

En la actualidad, el uso de la subred 0 y de la subred de sólo números 1 está generalmente aceptado y la mayoría de los fabricantes respalda su uso. Sin embargo, en ciertas redes, particularmente en las redes que utilizan software de legado, el uso de la subred 0 y de la subred de sólo números 1 todavía puede ocasionar problemas.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Asignar las direcciones dentro de una sección de la red del estadio.

Actividad en el laboratorio:

Refiera a la **actividad de laboratorio** del curso en línea

Crear una hoja de cálculo para la ubicación de la dirección para la red de CompañíaCinematográfica.

6.2.6 Diseño de un esquema de denominación

Refiera a la **Figura** del curso en línea

Los nombres de los dispositivos de red suelen asignarse en forma arbitraria. No se considera mucho su esquema o la información que contienen. Un buen esquema de denominación en la red facilita la administración de la misma y su uso por parte de los usuarios.

Existen dos tipos principales de nombres de red que se asignan:

- **Nombres de dispositivos internos**: solamente los administradores pueden ver estos nombres. Los nombres de router y switch son ejemplos de dispositivos internos.
- **Nombres externos**: los usuarios de la red pueden ver estos nombres. Un ejemplo es el nombre del dispositivo Windows que puede visualizarse en el entorno de red. Los nombres DNS también son nombres externos.

Pautas para la denominación

El sentido común suele determinar un esquema de denominación. Un buen esquema de denominación cumple con estas pautas:

- Mantener los nombres lo más cortos posibles; se recomienda menos de doce caracteres.
- Indicar el tipo de dispositivo, el objetivo y la ubicación con códigos, en lugar de utilizar palabras o abreviaturas.
- Mantener un esquema congruente. Esto facilita seleccionar y realizar informes de los dispositivos y configurar los sistemas de administración.
- Documentar los nombres en los archivos del departamento de TI y en los mapas de la red.
- Evitar nombres que facilite la ubicación de los recursos protegidos.

Los piratas informáticos pueden a veces obtener la suficiente información sólo de los nombres de la red para así encontrar los objetivos y explotar las vulnerabilidades conocidas. Se puede realizar una concesión para los nombres DNS externos, que deben ser fáciles de recordar y utilizar.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio:

Diagramar la nueva red de CompañíaCinematográfica e incluir los dispositivos, nombres de los dispositivos y direccionamiento IP.

6.3 Descripción de IPv4 e IPv6

6.3.1 Comparación de las direcciones de IPv4 e IPv6

Refiera a la **Figura** del curso en línea

El espacio de direcciones IPv4 proporciona aproximadamente 4.3 mil millones de direcciones. De dicho espacio de direcciones, aproximadamente 3.7 mil millones de direcciones son realmente asignables. Las otras direcciones se reservan para casos especiales como ***multicast***, espacio de direcciones privadas, loopback de prueba, e investigación. Hay pocos rangos de dirección IPv4 disponibles para asignar. Algunos ISP están comenzando a repartir asignaciones de dirección IPv6.

Una dirección IPv6 es un valor binario de 128 bits, que puede mostrarse como 32 dígitos ***hexadecimales***. Proporciona direcciones IP de 3.4 X 10^{38}.

Refiera a la **Figura** del curso en línea

El IPv6 ofrece potentes mejoras sobre el IPv4. Las mejoras incluyen:

- Movilidad y seguridad
- Encabezado más simple
- Formato de dirección

Movilidad y seguridad

La movilidad permite a las personas que tienen dispositivos de red móviles desplazarse por las redes. ***IP móvil*** es un estándar IETF que está disponible tanto para IPv4 como para IPv6. Este estándar permite a los dispositivos móviles trasladarse sin interrupciones en las conexiones de red establecidas. El IPv4 no admite este tipo de movilidad. La movilidad es una característica de IPv6.

IPSec es el estándar IETF para la seguridad de la red IP. Está disponible tanto para IPv4 como para IPv6. Las funciones de seguridad de la red IP son esencialmente idénticas en ambos entornos. IPSec está más estrictamente integrado al IPv6 y puede habilitarse en todos los nodos IPv6.

Encabezado más simple

El encabezado que se utiliza para IPv6 aumenta la eficiencia de enrutamiento al reducir el número de entradas en las tablas de enrutamiento.

No se asocian broadcasts al IPv6. Con el IPv4, los broadcasts creados generan un alto nivel de tráfico dentro de la red. Este tráfico crea un evento que se conoce como una tormenta de broadcast y toda la red deja de funcionar. El IPv6 reemplaza los broadcasts con multicasts y anycasts.

Refiera a la **Figura** del curso en línea

Formato de dirección

Los dos puntos separan las entradas en una serie de ocho campos hexadecimales de 16 bits que representan las direcciones IPv6. Los dígitos hexadecimales A, B, C, D, E y F que se representan en las direcciones IPv6 no distinguen mayúsculas de minúsculas.

A diferencia de IPv4, el formato de cadena de la dirección IPv6 no es fijo. Para las notaciones de cadena de direcciones IPv6 se utilizan las siguientes pautas:

- Los ceros al inicio en un campo son opcionales: 09C0 es igual a 9C0 y 0000 es igual a 0.
- Uno o más grupos de ceros pueden omitirse y reemplazarse por "::". Sólo se permite un "::" en la dirección.

- Una dirección no especificada se escribe como "::" porque contiene sólo ceros.

El uso de la notación "::" reduce en gran parte el tamaño de la mayoría de las direcciones. Por ejemplo, FF01:0:0:0:0:0:0:1 se transforma en FF01::1. Este formato contrasta con la notación decimal de 32 bits de IPv4. El principal tipo de dirección IPv6 se denomina ***unicast***.

Unicast envía paquetes a un dispositivo específico con una dirección específica. Multicast envía un paquete a todos los miembros de un grupo. Las direcciones anycast envían un paquete a cualquier miembro del grupo de dispositivos que tenga una dirección anycast asignada. Para fines de la eficiencia, un paquete que se envía a una dirección anycast se entrega a la interfaz más cercana. Por esa razón, anycast puede también considerarse como un tipo de dirección "de uno para el más cercano".

Refiera a la **Figura** del curso en línea

Los tipos básicos de direcciones IPv6 unicast son:

- Global
- Reservado (privado, loopback, no especificado)

Direcciones unicast globales

El host IPv6 es el equivalente de una dirección de host IPv4 registrada. Las direcciones de host IPv6 registradas se denominan direcciones unicast globales. El bloque de dirección unicast global se estructura para habilitar el agregado de los ***prefijos de enrutamiento***. Este agregado reduce la cantidad de entradas en la tabla de enrutamiento. Las direcciones unicast globales se agregan hacia arriba a través de organizaciones y eventualmente hacia los ISP.

Direcciones reservadas

IETF reserva una porción del espacio de direcciones IPv6 para distintos usos. A diferencia de IPv4, el IPv6 admite una mayor cantidad de direcciones reservadas. El IPv6 reserva 1/256 del total del espacio de direcciones IPv6. Algunos de los otros tipos de direcciones IPv6 provienen de este bloque, como las direcciones loopback y privadas.

Al igual que con IPv4, se separa un bloque de direcciones IPv6 para las direcciones privadas. Las direcciones privadas tienen un valor de FE en notación hexadecimal para el primer octeto. El próximo dígito hexadecimal es un valor de 8 a F.

6.3.2 Migración de IPv4 a IPv6

Riqueza en la transición

Refiera a la **Figura** del curso en línea

Hay varias formas de integrar una estructura IPv6 en una red IPv4 existente. La transición de IPv4 a IPv6 no tiene que hacerse toda al mismo tiempo. Los tres métodos de transición más comunes son:

- ***Stack doble***
- ***Tunneling***
- Uso de proxy y traducción

En el método de transición de stack doble se implementan ambas configuraciones IPv4 e IPv6 en un dispositivo de red. Ambos stacks de protocolos se ejecutan en el mismo dispositivo. Este método permite que IPv4 e IPv6 coexistan.

Tunneling es una técnica que se está haciendo más prominente a medida que IPv6 se adopta cada vez más. Tunneling es la encapsulación de un paquete de protocolo dentro de otro protocolo. Por ejemplo, un paquete IPv6 puede encapsularse dentro de un protocolo IPv4. Existe una variedad de métodos de tunneling de IPv6 sobre IPv4. Algunos métodos requieren la configuración manual y otros una más automática.

Las versiones 12.3(2)T y posteriores del software IOS de Cisco incluyen la traducción de direcciones de red y la traducción de protocolos (***NAT-PT***, Network Address Translation-Protocol Translation) entre IPv6 e IPv4. Esta traducción permite la comunicación directa entre los hosts que utilizan distintas versiones del protocolo IP.

Una migración global total de IPv4 a IPv6 puede no suceder en un futuro cercano. Sin embargo, ya se ha integrado en partes del mundo que ya casi han agotado sus direcciones IPv4.

6.3.3 Implementación de IPv6 en un dispositivo Cisco

Refiera a la **Figura** del curso en línea

De manera predeterminada, en un router Cisco se inhabilita el envío de tráfico IPv6. Para activar IPv6 en un router, siga estos dos pasos básicos:

Paso 1: Active el envío de tráfico IPv6 mediante el comando de configuración global **`ipv6 unicast-routing`**.

Paso 2: Configure las interfaces para que admitan el IPv6.

Los identificadores de interfaz en las direcciones IPv6 se utilizan para identificar las interfaces en un enlace. Se pueden considerar como la porción de host de una dirección IPv6. Los identificadores de interfaz deben ser únicos, siempre de 64 bits, y pueden derivarse en forma dinámica desde la encapsulación y los medios de Capa 2.

El comando de dirección IPv6 puede configurar una dirección IPv6 global. La totalidad de la dirección IPv6 de 128 bits puede especificarse mediante el comando **`ipv6 address`** *`dirección-ipv6/longitud_de_prefijo`*:

```
RouterX(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
```

Otra opción es configurar el identificador ***EUI-64*** para la porción de red de la dirección. El identificador de host es la porción de host de la dirección en el formato EUI-64 en una red Ethernet y es la dirección MAC del dispositivo. El método EUI-64 utiliza el comando **`ipv6 address`** *`prefijo_ipv6/longitud_de_prefijo`* **`eui-64`**:

```
RouterX(config-if)# ipv6 address 2001:DB8:c18:1::/64 eui-64
```

Refiera a la **Figura** del curso en línea

Si es necesario configurar un router en forma local para resolver los nombres de host a las direcciones IPv6, utilice el comando **`ipv6 host`** *`name ipv6addr`*.

Para especificar un servidor DNS externo que resuelva las direcciones IPv6, utilice el comando **`ip name-server`** *`dirección`*.

La configuración de la resolución de nombres en un router se hace por la comodidad de un técnico que utiliza el router para acceder a otros dispositivos en la red a través del nombre. No afecta el funcionamiento del router y no publica este nombre de servidor DNS a los clientes DHCP.

Refiera a la **Figura** del curso en línea

Configuración y verificación de RIPng para IPv6

La sintaxis que se utiliza para configurar RIPng para IPv6 es similar a la de IPv4, pero hay diferencias importantes. IPv4 utiliza el comando **`network`** para identificar qué interfaces se incluyen en la actualización de enrutamiento. IPv6 utiliza el comando **`ipv6 rip`** *`etiqueta`* **`enable`** en el modo de configuración de la interfaz para habilitar RIPng en una interfaz.

El parámetro *`etiqueta`* que se utiliza para el comando **`ipv6 rip enable`** debe coincidir con el parámetro *`etiqueta`* del comando **`ipv6 router rip`**.

Para verificar la configuración de RIP utilice el comando **`show ipv6 rip`** o el comando **`show ipv6 route rip`**. Habilitar RIP en una interfaz crea automáticamente un proceso rip de router según se necesite.

Refiera a la
Figura
del curso en línea

RIPng para la configuración de IPv6

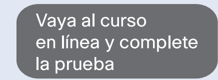
La configuración de routers que están directamente conectados habilita el uso del comando **`ipv6 rip`** *`nombre`* **`enable`**.

Por ejemplo, si dos routers están conectados en una red, ambos utilizan la etiqueta *`RT0`* para identificar el proceso RIPng. RIPng se habilita en la interfaz Ethernet de los routers que utilizan el comando**`ipv6 rip RTO enable`**.

Refiera al
Gráfico Interactivo
del curso en línea

Actividad en pantalla completa

Resumen del capítulo



Examen del capítulo

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 7

Creación de un prototipo de red

Introducción

Refiera a la **Figura** del curso en línea

7.1 Construcción de un prototipo para validar un diseño

7.1.1 Propósito de un prototipo

Prototipos y pilotos

Refiera a la **Figura** del curso en línea

Se recomienda como práctica probar todo diseño nuevo antes de aprobarlo e implementarlo. La comprobación proporciona una ***prueba de concepto*** para el diseño. La fase de prueba brinda la oportunidad de identificar las partes del diseño que no funcionan en forma adecuada y de volverlas a diseñar.

La red propuesta para el estadio incluye muchos cambios en el diseño. Por lo tanto, el diseñador de CompañíadeRedes prueba la función de las áreas críticas del diseño antes de crear la propuesta final.

Hay dos métodos comunes que se utilizan para probar un diseño de red:

- **Construcción de una red prototipo**: una red prototipo consta sólo de la porción de la red necesaria para probar una función o capacidad específica. Las redes prototipo están separadas de la red existente.
- **Instalación de una red piloto**: una prueba piloto comprueba la nueva funcionalidad o capacidad utilizando una porción de la red existente.

Ambos métodos prueban las funciones del diseño que afectan la capacidad que tiene la red para cumplir con los objetivos comerciales de alta prioridad.

Refiera a la **Figura** del curso en línea

Elección entre una prueba piloto o un prototipo

La decisión de crear un prototipo o realizar una prueba piloto depende de estos factores:

- El tipo de prueba requerido
- La posible interrupción de una prueba piloto en la red existente

Los prototipos suelen ser fáciles de configurar y controlar porque no afectan a ningún usuario de la red activa. En las redes prototipo, es fácil desconectar un dispositivo, hacer cambios de configuración o de hardware y volver a hacer la prueba en distintas condiciones. En una prueba piloto, este tipo de actividad puede ocasionar interrupciones importantes en la red.

¿Cuándo se debe crear una prueba piloto?

Mediante prototipos, se pueden probar muchas funciones de la red propuesta. Sin embargo, usar una prueba piloto es una buena opción en las siguientes circunstancias:

- **Cuando el prototipo no es lo suficientemente grande como para comprobar la funcionalidad**: comprobar el funcionamiento de un protocolo de enrutamiento en una red con cien routers puede no ser factible con un prototipo.
- **Cuando el desempeño de la red depende del funcionamiento de un dispositivo o tecnología de terceros específicos**: un ejemplo es un marcador de video costoso o un enlace WAN provisto por terceros.

El único cambio de diseño importante que requiere una prueba piloto es la instalación de la conexión Frame Relay en los sitios remotos. Una prueba piloto es una buena opción para probar esta conexión porque comprueba la calidad de la conexión actual y la funcionalidad y la configuración del dispositivo.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Observar las situaciones de red y decidir si es más adecuado un prototipo o una prueba piloto. Haga clic en la columna Prototipo o Piloto para cada una de las situaciones y luego haga clic en Verificar.

7.1.2 Creación de un plan de prueba

La construcción de un prototipo para probar un diseño de red requiere de una esfuerzo considerable de planificación. El diseñador de red crea un plan de prueba antes de iniciar el proceso para asegurar que los objetivos de la prueba sean claros y mensurables. Un plan de prueba es un documento que contiene varias secciones.

7.1.3 Verificación para comprobar si el diseño cumple con los objetivos y requisitos

Refiera a la **Figura** del curso en línea

Beneficios de la creación de un prototipo

La comprobación del diseño con una red prototipo cumple una función importante. Demuestra al cliente y al diseñador de red que el diseño de red cumple con los objetivos y los requisitos técnicos de la empresa. Crea una oportunidad para comparar las diferentes opciones de diseño y ver cuál funciona mejor.

Antes de iniciar las pruebas para verificar la funcionalidad del diseño específico, el personal de CompañíadeRedes construye y verifica la red prototipo en el plan de prueba. El diseñador entonces trabaja con el personal de CompañíadeRedes para configurar y llevar a cabo el plan de prueba. Analizan los métodos para medir las funciones de red prototipo en distintas condiciones.

Refiera a la **Figura** del curso en línea

Conectividad básica

Luego de conectar todo el equipo, el personal prueba la red prototipo para asegurar que proporcione conectividad básica. La conectividad básica se logra cuando la red funciona y los dispositivos envían y reciben datos. La verificación de la conectividad básica suele no ser parte del plan de pruebas formal. Sin embargo, esta verificación asegura que el diseñador tiene una red que funciona antes de realizar otras pruebas.

Los métodos que se utilizan para verificar la conectividad básica incluyen:

- Inspección visual de los indicadores LED en las NIC y en los dispositivos de redes.
- Uso de conexiones de consola a dispositivos para verificar el estado de las interfaces.

- Uso de los comandos **show** para proporcionar información sobre los dispositivos que tienen conexión directa. Los comandos **show** del router que comúnmente se utilizan para ver los dispositivos con conexión local son **show cdp neighbors** y **show ip arp**.

Refiera a la **Figura** del curso en línea

Prueba de funcionalidad

Cuando la configuración del prototipo esté completa, podrá comenzar la prueba de funcionalidad. Los objetivos de la empresa determinan los tipos de pruebas que se ejecutan en la red. El diseñador de red alinea cada objetivo comercial con los requisitos técnicos. Cuando realiza esto, ayuda a determinar el mejor método para demostrar las capacidades de la red.

Selección de un método de prueba

Los principales objetivos de la administración del estadio son mejorar la experiencia del cliente y garantizar la seguridad del cliente cuando asista a un evento al estadio.

Uno de los requisitos técnicos que respalda estos objetivos es la integración de la red de vigilancia con cámaras de seguridad en la LAN del estadio.

Para demostrar esta funcionalidad, se debe visualizar el video de vigilancia desde una PC ubicada en un segmento diferente de la red. El prototipo debe mostrar que sólo las estaciones autorizadas pueden visualizarlo. El diseñador enumera lo que debe suceder para lograr este objetivo:

- Crear VLAN de la capa de acceso para aislar el video de vigilancia del resto del tráfico de red.
- Implementar una estructura de dirección IP que admita las VLAN de la red de video.
- Realizar enlaces troncales desde las VLAN hasta los dispositivos de la capa de distribución.
- Pasar los flujos de video al servidor de vigilancia con video.
- Configurar las ACL para que el personal autorizado, pero no los usuarios visitantes, pueda ver el video de seguridad desde otras áreas del estadio.
- Implementar un mecanismo de autenticación en el servidor de vigilancia con video para asegurar que sólo los usuarios autorizados tengan acceso a los videos de seguridad.

El diseñador crea una lista de verificación para asegurar que la instalación y configuración de la red sea correcta. Cada uno de los elementos debe funcionar correctamente o la prueba de desempeño de extremo a extremo fallará.

7.1.4 Validación de los dispositivos y tecnologías de LAN

Refiera a la **Figura** del curso en línea

Existen herramientas comunes disponibles para analizar el rendimiento de la red prototipo.

Comandos Cisco IOS

Muchos aspectos del funcionamiento y rendimiento de la red pueden observarse mediante los comandos del software Cisco IOS: **show** y **debug**. Los comandos **show** muestran el estado actual de las interfaces, protocolos, tablas de enrutamiento, CPU, uso de la memoria y muchas otras variables. Los comandos **debug** permiten que el diseñador de red y el personal de CompañíadeRedes vean el procesamiento de la información en tiempo real. Las funciones de registro del software guardan y muestran información valiosa para un análisis posterior.

Herramientas y utilidades IP

Dos de los más conocidos comandos para la comprobación de posibilidad de conexión y conectividad de la red son **ping** y **traceroute**. Hay muchas otras utilidades y herramientas que pueden ayudar a determinar la funcionalidad de la red. Por ejemplo, en una PC con Windows, **netstat**, **nslookup**, **arp** y **telnet** pueden probar la conectividad y mostrar la información desde la PC.

Analizadores de protocolo

En un prototipo, los analizadores de protocolo verifican que los paquetes y las tramas contengan la información correcta. Los analizadores de protocolo ayudan a detectar la presencia de ciertos tipos de tráfico, tales como broadcast y ARP, que son difíciles de identificar sin examinar los datos a nivel de paquete o de trama.

Refiera a la **Figura** del curso en línea

Algunas veces es necesario comprobar la funcionalidad de la red en un entorno que la red prototipo no pueda duplicar. En este caso, el diseñador de red puede utilizar una herramienta de simulación de red.

Herramientas de simulación de red

Las herramientas de software pueden probar conceptos en un entorno simulado de manera similar a la herramienta Packet Tracer de Networking Academy con licencia que se utiliza en este curso. Las configuraciones o topologías de red pueden crearse o modificarse rápidamente. Las simulaciones pueden probar redes que son demasiado grandes como para que crear prototipos de las mismas.

Las mismas utilidades, herramientas IP e IOS que se utilizan en la red prototipo real pueden utilizarse para probar la red simulada.

El diseñador y el personal de CompañíadeRedes determinan las herramientas apropiadas a utilizar en cada prueba para demostrar la funcionalidad de la red. Por ejemplo, **`traceroute`** es una herramienta muy útil para mostrar la trayectoria de la ruta que un paquete sigue a través de una red. Sin embargo, no es una buena herramienta para demostrar la configuración para la sumarización de ruta.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Utilizar el software Cisco IOS y los comandos de Windows. Determine si esos comandos proporcionan la información necesaria para probar la funcionalidad de la red. Esta actividad se basa en una red prototipo previamente configurada.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Hacer coincidir la herramienta de prueba con el tipo de información que proporciona.

Nota: Se permite arrastrar las herramientas a más de una casilla. Se permite arrastrar varias herramientas a cada casilla.

7.1.5 Prueba de redundancia y capacidad de recuperación de la red

Superación de las fallas de enlace y de dispositivo

Refiera a la **Figura** del curso en línea

Cuando una empresa agrega aplicaciones que necesitan de una alta disponibilidad, el diseñador de red agrega redundancia a la red. Algunas veces, esta redundancia se agrega sin considerar lo que sucede durante una falla de red real. Es importante probar cómo funcionan los enlaces redundantes durante una situación de falla. Las pruebas deben medir cuánto tarda una red en estabilizarse después de que se activa el enlace redundante.

Enlaces redundantes

Los diseños de prototipo utilizan diferentes tipos de enlaces redundantes para probar la disponibilidad de la red. Los enlaces redundantes pueden utilizarse para la conmutación por error y algunas veces para el balanceo de carga durante el funcionamiento normal.

Balanceo de carga

No todos los tipos de enlaces redundantes admiten el balanceo de carga. Debido al funcionamiento del STP, los enlaces redundantes simples entre los switches de Capa 2 no pueden utilizarse para el balanceo de carga. Los enlaces enrutados del mismo costo y los enlaces de Capa 2 y 3 que se configuran como parte de un EtherChannel pueden utilizarse para balancear la carga de tráfico durante el funcionamiento normal. También pueden reenviar tráfico en caso de que se produzca una falla del enlace.

La red del estadio tiene dos tipos de enlaces redundantes entre los dispositivos: los uplink de Capa 2 y los enlaces de Capa 3 de igual costo.

Para probar los dos tipos de enlaces, el diseñador y el personal de CompañíadeRedes introducen fallas de enlace en la topología. Observando la cantidad de interrupciones en el servicio de red, se puede determinar cuánto tarda la red en volver a su estado de funcionalidad normal.

7.1.6 Identificación de riesgos o debilidades en el diseño

Refiera a la **Figura** del curso en línea

Los prototipos y las simulaciones pueden utilizarse para identificar los riesgos y las debilidades inherentes al diseño de la red. Una debilidad es un límite o un defecto en el diseño. Los riesgos son problemas adversos que pueden producirse a causa de una debilidad. Los riesgos aumentan cuando hay áreas en la red que no tienen un diseño óptimo. Estos límites pueden deberse a restricciones del equipo o a límites identificados anteriormente.

Algunas debilidades posibles del diseño y sus riesgos asociados incluyen:

- **Puntos únicos de falla**: en las áreas en donde hay redundancia limitada o donde no hay redundancia para proporcionar conectividad, existe el riesgo de que la falla de un único dispositivo o enlace puedan afectar toda el área.
- **Grandes dominios de fallas**: si un punto único de falla, tal como una conexión a Internet no redundante, afecta de manera adversa a una amplia porción de la red, aumenta el riesgo de que dicha falla tenga un impacto importante en la empresa.
- **Posibles cuellos de botella**: algunas áreas pueden ser vulnerables a la congestión si aumentan los volúmenes de tráfico, lo cual ocasiona un riesgo de degradación severa en el tiempo de respuesta.
- **Escalabilidad limitada**: las áreas o los dispositivos pueden presentar problemas de escalabilidad si la red crece más rápidamente de lo anticipado. La falta de escalabilidad puede requerir un rediseño de la red o una actualización costosa.
- **Capacidades del personal existente**: los prototipos a veces indican que las configuraciones de red son demasiado complejas para que el personal existente resuelva problemas y brinde soporte técnico. En casos como éste, hay riesgo mientras el personal no haya recibido la capacitación correspondiente o hasta que se haya implementado una nueva estrategia de soporte.

Deben comunicarse al cliente las debilidades identificadas por el diseñador de red y el personal de CompañíadeRedes durante la fase de prueba. Además, es importante incluir los riesgos que pueden estar asociados con las debilidades identificadas. Si se informan los riesgos, el cliente puede prever lo que podría ocurrir en el futuro y formular planes de contingencia sobre cómo manejar estas situaciones si se presentaran.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Analizar un plan de prueba de muestra y realizar la prueba.

7.2 Creación de un prototipo para la LAN

7.2.1 Identificación de los objetivos y requisitos que cumple el diseño de la LAN

Comprobación del nuevo diseño

Refiera a la **Figura** del curso en línea

Un objetivo comercial de alta prioridad para la administración del estadio es reducir los costos por medio de la implementación de una red convergente que admita tráfico de datos, telefonía IP y vigilancia por video. Como resultado, el nuevo diseño incorpora cambios importantes a la LAN del estadio. El diseñador de red debe decidir cómo probar los distintos elementos del diseño para asegurar que se cumplan los objetivos de la actualización de la red. El diseñador decide probar el diseño a través de una red prototipo.

¿Qué necesita probarse?

El diseñador debe decidir primero qué funciones de red necesitan incluirse en la prueba de prototipo. Ya que el objetivo es crear una red que admita tráfico de datos, telefonía IP y vigilancia por video, es necesario probar los elementos del diseño que tienen un impacto directo sobre dicho objetivo.

En la red del estadio, estos elementos son:

- La conversión de una red plana a una jerarquía modular de tres capas
- La creación de VLAN separadas y subredes IP para respaldar los distintos tipos de tráfico y clases de usuario
- La implementación de una topología redundante
- La configuración de las ACL para garantizar que sólo el personal autorizado tenga acceso a los recursos del estadio

7.2.2 Creación del plan de prueba

Refiera a la **Figura** del curso en línea

Luego de decidir qué objetivos comerciales y requisitos técnicos pueden comprobarse utilizando un prototipo de la red, el diseñador de red crea el plan de prueba.

El plan de prueba

El diseñador necesita demostrar la funcionalidad de la red convergente combinando el tráfico de datos, de telefonía IP y la vigilancia por video. Para hacer esto, el diseñador debe decidir:

- Qué tipos de prueba ejecutar
- Qué partes de la red deben construirse para realizar las pruebas
- Cómo determinar el éxito o la falla de la prueba

El diseñador enumera los resultados de la prueba que indican que se puede cumplir el objetivo de una red convergente. El objetivo específico de la prueba es mostrar de qué manera la nueva red cumple con el principal objetivo comercial. El personal de CompañíadeRedes prueba los requisitos técnicos individuales para determinar si el diseño de red cubre todos los objetivos. Repiten este proceso para cada uno de los objetivos de alta prioridad.

Prueba utilizando una topología de muestra

Refiera a la **Figura** del curso en línea

El diseñador de red crea una topología prototipo de prueba para el estadio, la cual es lo suficientemente grande como para demostrar el funcionamiento de la red planificada.

Simulación de una jerarquía de tres capas

Para cumplir con el objetivo del prototipo, la jerarquía de tres capas puede simularse usando dos dispositivos de Capa 2 y cuatro dispositivos de Capa 3. El diseñador selecciona los switches de

Capa 2 para simular la capa de acceso y utiliza los routers o switches de Capa 3 para simular las capas núcleo y de distribución. El diseñador hace una lista de todos los dispositivos y posibles sustitutos en el plan de prueba.

Para asegurar que la red prototipo está correctamente construida, el diseñador crea una lista de verificación que el personal de CompañíadeRedes deberá seguir. La lista de verificación incluye todas las funciones que deben funcionar cuando comience la prueba. Incluye todos los cambios planificados de las configuraciones que deben realizarse durante la prueba actual.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Realizar la prueba de conectividad básica en una red prototipo. Cree una lista de verificación con los criterios de éxito.

Se debe descargar este documento para realizar la actividad de Packet Tracer:

1. Plan de prueba prototipo del estadio.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un plan de prueba utilizando el diseño de red de CompañíaCinematográfica.

Se debe descargar este documento para realizar esta actividad en el laboratorio:

1. Plan de prueba de diseño de la LAN.

7.2.3 Validación de la elección de dispositivos y topologías

Refiera a la **Figura** del curso en línea

La red del estadio existente es una red conmutada, plana, sin enrutamiento ni filtrado. El diseñador de red propone incorporar servicios jerárquicos de Capa 3 además de la conmutación de Capa 2. El diseño propuesto incluye las capas núcleo y de distribución de la red. El diseñador recomienda estos cambios para atender los requisitos de escalabilidad y disponibilidad.

Topologías planas versus enrutadas

El diseñador quiere demostrar las diferencias entre las topologías planas y jerárquicas cuando se producen fallas de enlace. Esta demostración ejemplifica por qué la topología jerárquica enrutada es una mejor opción.

El diseño jerárquico modular propuesto para la red nueva permite agregar los módulos de la capa de acceso sin afectar a los usuarios existentes. Para demostrar esto correctamente, se debe construir un prototipo grande. Como esto no resulta práctico, el diseñador decide utilizar una herramienta de simulación en lugar de un prototipo para ejemplificar este beneficio potencial. La herramienta de simulación ayuda a validar la elección de una topología jerárquica enrutada.

El diseñador crea un plan de prueba para la simulación idéntico al que se hubiese escrito para una red prototipo.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Siguiendo un plan de prueba, comparar la forma en que las redes jerárquicas conmutadas y enrutadas se estabilizan luego de una falla de enlace importante.

Se deben descargar estos documentos para realizar la actividad de Packet Tracer:

1. Plan de prueba de redundancia del estadio

2. Lista de verificación para la instalación

7.2.4 Validación de la elección del protocolo de enrutamiento

Prueba del protocolo de enrutamiento

Refiera a la **Figura** del curso en línea

El diseño jerárquico de la red propuesta para el estadio incluye al EIGRP como protocolo de enrutamiento dinámico. El diseñador de red recomienda configurar el protocolo de enrutamiento dinámico EIGRP porque es fácil de utilizar y tiene buena capacidad de ampliación. EIGRP es un protocolo patentado y no puede configurarse en dispositivos que no sean de Cisco.

Es difícil demostrar con una red prototipo qué tan bien converge un protocolo de enrutamiento en caso de que se produzca una falla de enlace y es arriesgado intentarlo en una red piloto. En una prueba piloto, un solo error de configuración en el protocolo de enrutamiento puede interrumpir toda la red. A causa de este riesgo, el diseñador decide utilizar el simulador para las pruebas del protocolo de enrutamiento.

El diseñador desea comparar el uso de las rutas estáticas para los enlaces redundantes con el uso del protocolo de enrutamiento EIGRP. El plan de prueba primero describe una prueba de las rutas estáticas y luego la configuración de EIGRP para que se pueda efectuar una comparación.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Siguiendo un plan de prueba, construir y comprobar una red de varios routers con enlaces redundantes.

Se deben descargar estos documentos para realizar la actividad de Packet Tracer:

1. Plan de prueba del protocolo de enrutamiento del estadio.

7.2.5 Validación del esquema de direccionamiento IP

Refiera a la **Figura** del curso en línea

El esquema de direccionamiento IP propuesto para utilizar en la red del estadio puede comprobarse por medio de la red prototipo. El diseñador de red recomienda utilizar una herramienta de simulación para comprobar el esquema de direccionamiento IP. Con la herramienta de simulación, el diseñador puede determinar si la estructura de direccionamiento habilita el resumen y puede admitir la escalabilidad necesaria.

El diseñador configura la red simulada con la misma cantidad de dispositivos de red que la red planificada. El diseñador valida entonces la ubicación de las distintas subredes y la configuración de la sumarización de ruta.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Aplicar un esquema de direccionamiento IP a un módulo de la capa de distribución de la LAN del estadio.

Se debe descargar este documento para realizar la actividad de Packet Tracer:

1. Plan de prueba de la dirección IP del estadio.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Construir la red prototipo de CompañíaCinematográfica. Realice las pruebas según el plan de prueba que se creó anteriormente en este capítulo.

Analice los resultados para determinar el éxito o las fallas. Complete la sección Resultados reales del plan de prueba.

7.2.6 Identificación de riesgos y debilidades

Registro de riesgos y debilidades

Refiera a la **Figura** del curso en línea

En la sección Conclusión del plan de prueba, el diseñador de red y el personal de CompañíadeRedes anotan las observaciones y opiniones sobre los resultados de la prueba. Una parte importante de esta sección es el análisis de los riesgos y debilidades del diseño. En el caso de la red propuesta para el estadio, hay algunos riesgos que se deben informar. La documentación de estos riesgos ayuda a la administración del estadio a tomar decisiones con fundamento acerca de la implementación del diseño.

Los riesgos y debilidades incluyen:

- **No hay redundancia en la capa de acceso de la red** : la mayoría de los dispositivos de los usuarios finales se conectan a un único switch de acceso. Éste es un único punto de falla para los dispositivos finales. Debido al mayor riesgo de pérdida del servidor, los servidores del centro de datos se conectan a NIC duales para separar los switches de acceso.
- **Un solo ISP para la conectividad de Internet**: si la conexión del ISP falla o si hay un problema en el ISP, se pierde toda la conectividad a Internet para la red del estadio.
- **Ancho de banda limitado para WAN e Internet**: cuando aumentan los requisitos para la WAN y la conectividad a Internet, los límites de ancho de banda pueden ocasionar un cuello de botella y reducir el rendimiento de las aplicaciones.
- **Conectividad de fibra limitada desde los armarios para el cableado**: a causa de esta restricción, la cantidad de enlaces redundantes desde los dispositivos de la capa de acceso se limita a dos. Por lo tanto, varios switches en un armario para cableado deben compartir los uplink.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Analizar los resultados de las pruebas de prototipo para determinar el nivel de riesgo en la red de CompañíaCinematográfica.

Complete la sección Conclusiones del plan de prueba.

7.3 Creación de un prototipo de la granja de servidores

7.3.1 Identificación de los objetivos y requisitos de la granja de servidores

Refiera a la **Figura** del curso en línea

Uno de los objetivos comerciales de la red del estadio es proporcionar un mejor servicio al cliente. Este objetivo puede lograrse mejorando el acceso al sitio Web para ver los horarios, comprar e imprimir boletos y comprar productos.

El diseño propuesto recomienda reubicar el servidor Web, el servidor DNS y el servidor de la base de datos en un conjunto de servidores ubicado en un nuevo centro de datos.

Reubicación del servidor para la red del estadio

La reubicación de estos servidores desde las oficinas de administración del estadio hasta un nuevo centro de datos es un cambio importante en la manera en que el tráfico fluye en la red del estadio. Es una pieza fundamental del diseño propuesto. Los requisitos de contar con casi un 100% del

tiempo de actividad y disponibilidad pueden cumplirse mejor si los servidores están ubicados en un centro de datos central. El diseño del centro de datos es un módulo de red que se puede comprobar en un prototipo.

7.3.2 Creación del plan de prueba

¿Qué necesita probarse?

Refiera a la **Figura** del curso en línea

En el diseño de red propuesto para el estadio, los siguientes elementos tienen un impacto directo sobre la granja de servidores:

- La creación de una topología modular de granja de servidores
- La implementación de enlaces redundantes para la conectividad del servidor
- La ubicación de los switches redundantes de Capa 2 para la conectividad del servidor
- El uso de un árbol de expansión rápido por VLAN para acortar el tiempo en que los enlaces conmutados redundantes se activan luego de una falla
- La configuración de una estructura de direccionamiento IP flexible
- La configuración de EIGRP en las capas núcleo y de distribución del centro de datos
- La configuración de estrictas políticas de filtrado de tráfico para evitar el acceso no autorizado

El diseñador de red decide construir una red prototipo. Dado que el diseñador no cuenta con switches disponibles de varias capas, se utilizan routers para desempeñar la función de Capa 3. La topología de red prototipo consta de cinco switches de Capa 2, cinco dispositivos de Capa 3 y una cantidad de PC que emulan los servidores que ejecutan las distintas aplicaciones. Mediante esta topología, el personal de CompañíadeRedes puede demostrar que los objetivos comerciales y los requisitos técnicos pueden cumplirse con el diseño propuesto.

Refiera a la **Figura** del curso en línea

El personal de CompañíadeRedes utiliza la lista de verificación creada por el diseñador de red para construir la red prototipo.

Prueba de la red prototipo

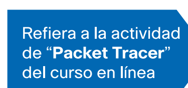
Luego de haber construido la red prototipo, el personal ejecuta las pruebas de conectividad básica para asegurar que la red esté configurada correctamente. Luego crean una línea de base de red.

Mediciones de la línea de base

Es importante desarrollar las mediciones de la línea de base de la red prototipo. Los resultados que se observan durante las distintas pruebas se comparan entonces con la configuración original. De esta manera, el personal puede identificar y registrar cualquier proceso o función que incrementa el uso del procesador o disminuye el ancho de banda disponible.

Para simular el tráfico en la red, el diseñador recomienda ejecutar un generador de tráfico en una de las PC conectadas. Un generador de tráfico es una herramienta de prueba que simula los distintos niveles de uso de la red. En el caso de un prototipo de granja de servidores, el diseñador intenta utilizar la herramienta para simular el tráfico de red hacia el servidor Web.

Actividad de Packet Tracer



Construir la red prototipo utilizando la lista de verificación creada por el diseñador de red. Realice la prueba de conectividad básica según el plan de prueba.

Se deben descargar estos documentos para realizar la actividad de Packet Tracer:

1. Plan de prueba de conectividad básica del estadio

2. Lista de verificación para la instalación

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un plan de prueba de la granja de servidores y una lista de verificación de la instalación del prototipo para CompañíaCinematográfica.

Se deben descargar estos documentos para realizar la actividad en el laboratorio:

1. Plan de prueba del diseño de la granja de servidores

2. Lista de verificación para la instalación

7.3.3 Validación de la selección de topología y dispositivo

Refiera a la **Figura** del curso en línea

El diseño propuesto para el centro de datos de la red del estadio utiliza una topología jerárquica redundante para la granja de servidores.

Simulación de la LAN

En las pruebas de simulación de la LAN, los enlaces enrutados usualmente convergieron más rápidamente que los enlaces STP en caso de que se produjera una falla. Por lo tanto, el diseñador de red elige realizar un prototipo de los enlaces conmutados con el protocolo rápido de árbol de expansión (***RSTP***, Rapid Spanning Tree Protocol) para comprobar la velocidad con la que se recupera de una falla la red de la granja de servidores. El diseñador revisa el funcionamiento del RSTP con los técnicos de red antes de configurar la prueba.

El RSTP proporciona una rápida conectividad después de la falla de un switch, un puerto del switch o una LAN. El RSTP habilita la configuración del puerto del switch para que los puertos puedan realizar la transición al envío directo cuando el switch se reinicia.

Protocolo rápido de árbol de expansión por cada VLAN

El estándar RSTP (802.1w) supone sólo una instancia de árbol de expansión para toda la red conmutada, independientemente de la cantidad de VLAN. La implementación de Cisco del RSTP es Árbol de expansión rápido plus por cada VLAN (PVRST+, Per VLAN Rapid Spanning Tree Plus). PVRST+ define un protocolo de árbol de expansión que tiene una instancia de RSTP por cada VLAN. La documentación de Cisco suele hacer referencia a esta implementación como RSTP.

Roles de los puertos

Refiera a la **Figura** del curso en línea

El RSTP define los siguientes roles de los puertos:

- ***De raíz:*** un puerto de envío seleccionado para cada switch que no es de raíz y que proporciona la ruta de menor costo hacia el switch de raíz.
- ***Designado:*** un puerto de envío elegido para cada segmento de LAN conmutado en base a la mejor unidad de datos del protocolo de puente (***BPDU***, bridge protocol data unit). Este puerto es la ruta de menor costo hacia el switch de raíz desde el segmento de LAN.
- ***Alternativo:*** una ruta alternativa hacia el switch de raíz para un switch que no es de raíz y que es diferente a la trayectoria que toma el puerto de raíz. Este puerto está bloqueado para el envío de tráfico.
- ***De respaldo:*** una ruta de respaldo que proporciona una conexión redundante, aunque menos deseable, hacia un segmento al que está conectado otro puerto del switch que no es de raíz. Este puerto está bloqueado. (Los puertos de respaldo sólo pueden existir cuando dos puertos se conectan juntos en un loopback por medio de un puente o enlace punto a punto con dos o más conexiones a un segmento de la LAN compartido).
- ***Inhabilitado:*** un puerto que no participa en el funcionamiento de árbol de expansión

Los roles de puertos designados y de raíz incluyen el puerto de la topología activa. Los roles de los puertos de respaldo y alternativos excluyen el puerto de la topología activa.

Red del estadio

Refiera a la **Figura** del curso en línea

El diseñador de red revisa el funcionamiento del RSTP con el personal de CompañíadeRedes. El diseñador crea una lista de verificación para la instalación y un plan de prueba para verificar que los enlaces conmutados pueden proporcionar la capacidad de recuperación requerida.

Siguiendo los detalles que se incluyen en la lista de verificación, el personal de CompañíadeRedes establece un árbol de expansión rápido por cada VLAN en los switches de la capa de acceso. El personal designa los puentes de raíz primarios y secundarios para asegurar que la red permanezca estable si se agregan nuevos switches a la topología. Después introducen fallas en la topología conmutada para observar los resultados.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastre el estado de puerto hacia el rol de puerto correspondiente y luego haga clic en Verificar.

Actividad en el laboratorio

Refiera a la **actividad de laboratorio** del curso en línea

Configurar y verificar RSTP en una red prototipo.

7.3.4 Validación del plan de seguridad

La disponibilidad y la seguridad son los dos requisitos primarios para la red de la granja de servidores del estadio.

Refiera a la **Figura** del curso en línea

Requisitos de disponibilidad

El diseñador de red se ocupa de los requisitos de disponibilidad utilizando componentes y enlaces redundantes donde sea posible. La configuración de RSTP para la Capa 2 y el uso de EIGRP para la Capa 3 asegura la rápida convergencia de la red en el caso de producirse una falla.

Seguridad de varias capas

El diseño propuesto para la granja de servidores implementa varias capas de seguridad. Las utilidades y los programas protegen los servidores contra ataques de virus y gusanos, y también proporcionan prevención de intrusión basada en el host. Los mecanismos de autenticación sólo permiten el acceso a usuarios autorizados.

En la capa de acceso, el uso de seguridad de puerto y la deshabilitación de los puertos no utilizados ayudan a prevenir el acceso no autorizado.

Las ACL filtran el tráfico y previenen que el tráfico de la ***suplantación de identidad*** o no solicitado que llegue a los servidores. Las ACL se colocan en el punto en donde la granja de servidores se conecta con la red del estadio.

Firewall

Los firewall y la función de firewall del software Cisco IOS proporcionan capacidad de firewall con estado. Los IPS protegen la red ante las amenazas conocidas y de los patrones de tráfico anormal.

Prueba del diseño de la ACL

Refiera a la **Figura** del curso en línea

El diseñador de red decide comprobar el diseño de la ACL y su ubicación porque tiene las mayores probabilidades de variabilidad. El diseñador crea un plan de prueba que enumera todas las reglas de filtrado y métodos de prueba. El diseñador sugiere utilizar un simulador de red en lugar de una

red prototipo. El simulador puede configurarse rápidamente para que contenga todos los enlaces y dispositivos propuestos.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Utilizando una red prototipo, aplicar y comprobar las ACL diseñadas para proteger la granja de servidores de la red del estadio de ataques y accesos no autorizados.

Se debe descargar este documento para realizar la actividad de Packet Tracer:

1. Plan de prueba de la ACL del estadio

7.3.5 Verificar si el diseño cumple con los objetivos comerciales

Actividad en el laboratorio

Refiera a la **actividad de laboratorio** del curso en línea

Construir la red prototipo de CompañíaCinematográfica y realizar las pruebas según el plan de prueba que se creó en la actividad en el laboratorio *Creación de un plan de prueba para la granja de servidores*.

Luego analice los resultados para determinar el éxito o la falla de las pruebas y complete la sección Resultados reales del plan de prueba.

7.3.6 Identificación de riesgos y debilidades

Refiera a la **Figura** del curso en línea

Al finalizar la prueba de simulación y de prototipo de la granja de servidores, se identifican algunas áreas problemáticas del diseño propuesto. El diseñador de red está satisfecho con el funcionamiento esperado de la red. Sin embargo, el estadio necesita considerar algunos cambios en el diseño a medida que la red crezca y madure.

Debilidades identificadas

Las pruebas muestran que las ACL y la capa de distribución evitan el ingreso del tráfico no autorizado a la granja de servidores, pero no son efectivas para filtrar el tráfico dentro de las VLAN. El tráfico de prueba entre los servidores de la misma VLAN no está restringido.

Recomendaciones

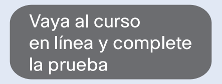
El diseño de red admite el crecimiento del centro de datos y de la granja de servidores. El diseñador recomienda que la administración del estadio considere utilizar switches de varias capas en la capa de acceso. Los switches de varias capas proporcionan más flexibilidad que los switches de Capa 2 para separar y filtrar el tráfico de los usuarios que se encuentran fuera del centro de datos. Además, los switches de varias capas proporcionan más flexibilidad que los switches de Capa 2 para separar y filtrar el tráfico de los dispositivos que se encuentran dentro del centro de datos.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Analizar los resultados de la prueba de prototipo de CompañíaCinematográfica y documentar todos los riesgos o debilidades del diseño. Complete la sección Conclusiones del plan de prueba.

Resumen del capítulo



Examen del capítulo

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 8

Creación del prototipo de la WAN

Introducción

Refiera a la **Figura** del curso en línea

8.1 Creación del prototipo de la conectividad remota

8.1.1 Descripción de los métodos de prueba de conectividad remota

Refiera a la **Figura** del curso en línea

Los resultados de la prueba prototipo de la LAN validan las opciones de diseño que eligió el diseñador de CompañíadeRedes. Se deben probar los elementos del nuevo diseño que proporcionan la conectividad WAN a trabajadores y sitios remotos. Puede ser más difícil probar las opciones de conectividad remota que el diseño de la LAN.

La conectividad remota usualmente requiere el uso de instalaciones de transmisión que no son de propiedad del cliente o que éste no administre. Estas instalaciones: redes Frame Relay, conexiones T1 o incluso enlaces DSL, no están usualmente disponibles para el diseñador a los fines de la prueba. Como resultado, el diseñador debe considerar formas de probar el diseño que se propone sin acceder a las instalaciones de transmisión actuales.

El diseñador puede utilizar tres métodos diferentes para probar los diseños de la conectividad remota:

- Software de simulación
- Pruebas prototipo mediante enlaces simulados
- Pruebas piloto en el entorno real

8.1.2 Prueba de la conectividad WAN con software de simulación

Refiera a la **Figura** del curso en línea

Los entornos simulados pueden proporcionar una forma de probar la configuración y el funcionamiento del dispositivo. Después de que el diseño se verifica en el entorno simulado, la conectividad remota puede además probarse en una instalación piloto.

Software de simulación de red

Los programas de software de computadora le ofrecen al diseñador una herramienta para probar las configuraciones antes de implementarlas en el equipo existente. Entre los beneficios de utilizar un paquete de software de simulación, se encuentran:

- **Menor costo total**: las redes de prueba son costosas para construir y mantener. Las capacidades del dispositivo de red y las opciones de configuración cambian frecuentemente. Como resultado, puede resultar difícil mantener un entorno de laboratorio actualizado.

- **Flexibilidad**: el software de simulación puede soportar muchos tipos de dispositivos y opciones de conectividad. El cambio de las configuraciones y topologías usualmente es mucho más rápido y fácil en una simulación que cuando se utiliza el equipo real.
- **Escalabilidad**: construir una red grande o compleja en un entorno de laboratorio lleva tiempo y está propensa a errores. El uso de un programa de simulación permite probar redes grandes en una cantidad de tiempo reducida.
- **Control**: el uso del software de simulación le permite al diseñador controlar simultáneamente todo el funcionamiento de la red. El diseñador de red puede determinar los tipos de tráfico que se envían a través de la red y la velocidad con la que se envían. El diseñador puede además detener la simulación para capturar y examinar los paquetes en distintos puntos de la red.

Refiera a la **Figura** del curso en línea

Límites del software

El uso de programas de software de simulación para validar los diseños de la red presenta algunas desventajas:

- **Funcionalidad limitada**: los programas de software se diseñan y escriben mucho antes de que estén a disposición del público. Además, pueden desactualizarse rápidamente. El software puede admitir sólo algunas de las capacidades del equipo actual.
- **Rendimiento poco realista**: es difícil, si no imposible, que los programadores de software anticipen y simulen todas las condiciones que se pueden dar en la red actual. Por lo tanto, es arriesgado confiar en las estimaciones de programación y rendimiento que se obtienen del software de simulación.

A pesar de estas desventajas, el uso del software de simulación para probar las configuraciones es una excelente manera de descubrir los errores de diseño.

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Actividad de Packet Tracer

Utilice Packet Tracer para simular una WAN serial con varios routers mediante PPP.

8.1.3 Simulación de la conectividad WAN en un entorno de laboratorio

Refiera a la **Figura** del curso en línea

Además del software de simulación de red, hay otros métodos disponibles para simular la conectividad remota en un entorno de prueba.

Casi todas las tecnologías WAN requieren un dispositivo intermediario para convertir las señales WAN a señales seriales o Ethernet en las instalaciones del cliente. Estos dispositivos incluyen distintos tipos de módems y ***CSU/DSU***. Una excepción es la red Metro Ethernet, la cual no requiere el dispositivo intermediario.

Simulación de DSL o conexión por cable

Para simular un DSL o una conexión WAN por cable, se puede utilizar una conexión Ethernet. La mayoría de las interfaces Ethernet se pueden configurar para proporcionar una conexión de 10 Mb, lo cual es similar al tipo de conectividad que se proporciona con DSL o por cable. Los routers se conectan mediante un ***cable de conexión cruzada*** Ethernet. Se puede ajustar la métrica del protocolo de enrutamiento para simular la métrica de un enlace de menor velocidad mediante el uso del comando `bandwidth` en la interfaz. La preferencia de ruta estática se puede configurar en forma manual mediante el ajuste de la ***distancia administrativa*** que se asigna a la ruta.

Refiera a la **Figura** del curso en línea

Simulación de la conectividad serial

Hay dos métodos comunes que se utilizan para simular la conectividad serial:

- CSU/DSU o módems seriales
- Cables V.35

Uso de CSU/DSU o módems

Si se encuentran disponibles CSU/DSU o módems, la documentación que se adjunta al dispositivo generalmente incluye el diagrama de cableado necesario para crear un cable de conexión cruzada. Si no se incluye el diagrama, el usuario puede buscar en Internet las salidas de pin correctas que deben usarse. Este cable de conexión cruzada puede utilizarse para conectar dos dispositivos similares para simular el enlace que proporciona el proveedor de servicios de telecomunicaciones (***TSP***).

Una CSU/DSU o un módem se configura para proporcionar la función ***DCE***. El otro dispositivo se configura como un dispositivo ***DTE***. Los routers entonces se conectan y se configuran como se conectarían y configurarían en el entorno WAN real. La CSU/DSU o el módem proporciona la temporización para el enlace.

Refiera a la **Figura** del curso en línea

Uso de cables V.35

En el entorno de laboratorio prototipo de CompañíadeRedes, es posible simular una conexión WAN punto a punto mediante el uso de dos cables seriales V.35. Uno de los cables debe ser un cable DCE V.35 y el otro debe ser un cable DTE V.35. Al conectar los dos cables, se crea un cable de conexión cruzada V.35. Al interconectar los routers con estos dos cables, se crea un circuito. Al eliminar la CSU/DSU o el módem de la conexión, se elimina la función de temporización del circuito. Como resultado, uno de los routers debe configurarse como un dispositivo DCE, mediante el uso del comando **`clock rate`** en la interfaz. En las implementaciones reales, los routers y otros dispositivos CPE rara vez, o nunca, proporcionan la función DCE en un circuito.

Al establecer las distintas frecuencias de reloj, el diseñador de red y el personal de CompañíadeRedes pueden realizar las pruebas para simular las distintas velocidades de conexión.

La ventaja de utilizar las conexiones WAN seriales simuladas es la posibilidad de probar y verificar la configuración de las interfaces seriales. La desventaja de realizar este tipo de prueba simulada es la imposibilidad de evaluar los factores de la red actual del proveedor de telecomunicaciones.

Luego de probar las configuraciones de manera simulada, se recomienda realizar pruebas adicionales mediante el uso de una instalación piloto.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Conectar dos routers con un DCE y un cable DTE v.35. Configure un dispositivo para proporcionar la temporización para la interfaz.

8.2 Creación de un prototipo para la conectividad WAN

8.2.1 Identificación de los requisitos y objetivos de la WAN

Refiera a la **Figura** del curso en línea

La conectividad a sitios remotos es un gran problema para la red del estadio existente. Un objetivo de alta prioridad para la administración del estadio es ampliar el nuevo sistema de telefonía IP y la red de vigilancia con video a los sitios remotos actuales. Estos servicios no pueden admitirse en la WAN existente.

En la red del estadio, los dos sitios remotos existentes acceden a la red principal con el uso de las conexiones de red privada virtual (***VPN***) a través de Internet. Estas conexiones VPN utilizan líneas DSL. El ISP no garantiza el ancho de banda o la calidad de servicio. El diseño que se propone incluye una actualización de la conectividad WAN Frame Relay dedicada. El diseñador de red recomienda utilizar Frame Relay para conectar la nueva oficina remota para el equipo A y la oficina de CompañíaCinematográfica.

Las VPN existentes a través de Internet permanecen en el nuevo diseño para respaldar la nueva WAN.

El diseñador decide construir un prototipo para simular la conectividad WAN. Este prototipo prueba las configuraciones y la conmutación por error en caso de que se produzca una falla de enlace. No es posible simular la totalidad de la red de conmutación por paquete del TSP al usar un prototipo o un software de simulación. La conexión Frame Relay existente a través de la red del TSP sólo puede comprobarse con una prueba piloto. Luego de completar el prototipo y aceptar el diseño, se planifica una instalación piloto para la tienda de recuerdos.

Refiera a la **Figura** del curso en línea

8.2.2 Creación del plan de prueba

El rendimiento a través de la red del TSP no puede comprobarse en el prototipo. Sin embargo, otros elementos importantes del diseño pueden comprobarse en la red WAN prototipo:

- Configuración del loop local de Frame Relay
- Los mecanismos para activar el enlace de respaldo de la VPN en caso de que se produzca una falla del Frame Relay
- Configuración del enrutamiento estático
- Las ACL que filtran el tráfico hacia y desde los sitios WAN
- Configuración de SSH para permitir la administración remota

Para crear un prototipo de la conectividad WAN, el diseñador de red recomienda utilizar un router Cisco para simular un switch Frame Relay. Esta simulación permite que se prueben las configuraciones de loop locales sin necesidad de conexión física a la red del TSP. Para construir el prototipo WAN, el diseñador necesita cuatro routers para probar todas las funcionalidades.

Refiera a la **Figura** del curso en línea

El diseñador crea el diagrama de topología de prueba, la lista de verificación para la instalación y el plan de prueba para demostrar la conectividad de Frame Relay.

La topología para la prueba WAN Frame Relay requiere de otro tipo de conectividad diferente a los prototipos anteriores. Durante una implementación real, un loop local de Frame Relay usualmente se conecta a una CSU/DSU en la instalación del cliente. Desde la CSU/DSU, se realiza una conexión serial hasta el router del equipo local del cliente (***CPE***).

La función DCE del bucle local proviene del TSP o de la CSU/DSU. La temporización para la conexión serial entre la CSU/DSU y el router CPE proviene de la CSU/DSU. Todas las conexiones en el router son conexiones DTE y utilizan un cable DTE.

En la red de prueba prototipo, no hay una conexión verdadera ***T1*** o ***E1*** a un switch Frame Relay. Debe simularse con un router Cisco para que actúe como el switch Frame Relay. Este router se identifica como FR1. Se conecta a los otros routers de la topología mediante una conexión cruzada. En CompañíadeRedes, esta función de conexión cruzada se logra mediante la conexión de un cable DTE V.35 directamente a un cable DCE V.35. Debido a que no existe una CSU/DSU en la topología de prueba, las interfaces del router FR1 se configuran con una velocidad de reloj para proporcionar la función DCE.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un plan de prueba para crear el prototipo de la conectividad WAN entre CompañíaCinematográfica y el estadio.

Se deberá descargar este documento para realizar la actividad en el laboratorio:

1. Plan de prueba de diseño de la WAN

8.2.3 Validación de la elección de dispositivos y topologías

Refiera a la **Figura** del curso en línea

La topología Frame Relay que se recomienda en el diseño WAN propuesto es sumamente diferente a la conectividad VPN existente que el ISP administra. Hay muchas opciones disponibles cuando se utiliza Frame Relay. Se recomienda como práctica que el diseñador de red revise el diseño y el funcionamiento de la WAN con el personal de CompañíadeRedes antes de que configuren el prototipo.

Frame Relay

Frame Relay es un protocolo WAN de alto rendimiento que normaliza la Unión Internacional de Telecomunicaciones ***ITU-T***. Se utiliza ampliamente en Estados Unidos. Mucha gente piensa que un enlace Frame Relay es una conexión física entre dos sitios. En realidad, un enlace Frame Relay es un circuito virtual que abarca una serie de conexiones.

Cada enlace Frame Relay tiene por lo menos tres componentes:

- El circuito punto a punto local que conecta el router CPE local al switch Frame Relay del TSP
- La red de conmutación por paquetes del TSP
- El circuito punto a punto remoto que conecta el sitio remoto en la red TSP

La configuración de Frame Relay en el router CPE consiste en configurar solamente los parámetros para el enlace punto a punto con el switch Frame Relay del TSP. Estos enlaces punto a punto usualmente son circuitos T1/E1 o T1/E1 fraccional. El TSP configura el circuito virtual a través de la red de conmutación por paquetes.

Refiera a la **Figura** del curso en línea

La configuración y la terminología Frame Relay pueden ser confusas. Para explicar las opciones de configuración al personal de CompañíadeRedes, el diseñador de red comienza con un enlace entre el nuevo router CPE que se planifica para el estadio y un switch Frame Relay del TSP.

El bucle local

La conexión propuesta entre el router CPE del estadio y el switch Frame Relay en el TSP es un circuito T1. Esta conexión se denomina un ***bucle local***. El bucle local conecta el switch Frame Relay del proveedor a la CSU/DSU de las instalaciones del estadio. La conexión luego termina en el puerto serial del router CPE. La velocidad del reloj (velocidad del puerto) de la conexión del bucle local a la nube Frame Relay se denomina ***velocidad de acceso local***. La velocidad de acceso local define la velocidad con la cual los datos entran y salen de la red de conmutación por paquete del proveedor, independientemente de otros parámetros.

Identificador de la conexión de enlace de datos

Se puede admitir más de un circuito virtual en un único circuito de bucle local físico. Cada extremo de circuito virtual se identifica con un identificador de conexión de enlace de datos (***DLCI***). Un DLCI suele ser importante sólo en el bucle local. En otras palabras, los números DLCI son exclusivos dentro de un único switch Frame Relay. Sin embargo, debido a que puede haber muchos switches Frame Relay en la red, los números DLCI pueden duplicarse en otros switches.

Refiera a la **Figura** del curso en línea

Algunos de los servicios que ofrece el switch Frame Relay afectan la calidad de las transmisiones de datos a través de la red del proveedor de telecomunicaciones.

Velocidades de datos garantizadas

Los proveedores de Frame Relay ofrecen servicios con velocidades de transferencia de datos promedio garantizadas a través de la red de conmutación por paquete del proveedor. Esta velocidad de información suscrita (***CIR***) especifica la velocidad de datos máxima promedio que brinda la red en condiciones normales. La CIR es menos que o igual a la velocidad de acceso local. Una CIR se asigna a cada DLCI que se transporta en el bucle local. Si el estadio intenta enviar datos a una velocidad mayor que la CIR, la red del proveedor señala algunos frames con un bit elegible para descarte (***DE***) en el encabezado de la dirección del frame. La red intenta entregar todas las tramas. Sin embargo, si hay saturación, la red descarta las tramas que el bit DE marca.

CIR cero

Muchos servicios Frame Relay económicos se basan en una CIR cero. Una ***CIR cero*** significa que cada trama es una trama DE y la red puede descartar cualquier trama cuando haya saturación. No hay garantía de servicio con una CIR que se establece en cero; por lo tanto, estos servicios no son una buena opción para los datos esenciales para el trabajo.

Interfaz de administración local

La interfaz de administración local (***LMI***) es un estándar de señalización entre el router (dispositivo DTE) y el switch Frame Relay local (dispositivo DCE). La LMI tiene la responsabilidad de administrar la conexión y mantener el estado entre el router y el switch Frame Relay. Por ejemplo, la LMI utiliza mensajes de ***actividad*** para monitorear el estado de las conexiones de red. Frame Relay de LMI agrega un conjunto de mejoras, que se conocen como extensiones, al Frame Relay básico. Una extensión importante de la LMI es la capacidad de informar el estado del circuito virtual y el estado de la conexión física. Los estándares de la LMI pueden diferir entre las redes. Los routers Cisco admiten tres tipos de LMI: Cisco, anexo D de ANSI y anexo A de UTI-T Q.933.

Refiera a la **Figura** del curso en línea

Control de congestión

Para ayudar a administrar el flujo de tráfico en la red, Frame Relay implementa dos mecanismos:

- Notificación explícita hacia adelante de congestión (***FECN***)
- Notificación de congestión explícita retrospectiva (***BECN***)

Las FECN y a las BECN las controla un único bit que se incluye en el encabezado de la trama de Frame Relay.

FECN

La FECN informa al dispositivo de destino que hay congestión en la ruta de la red. El bit de la FECN forma parte del campo Dirección en el encabezado de la trama de Frame Relay. El mecanismo FECN funciona de la siguiente manera:

1. Un dispositivo DTE envía frames de Frame Relay a la red.

2. Si la red se congestiona, los dispositivos DCE (switches) establecen el valor del bit de la FECN en 1.

3. Los frames llegan al dispositivo DTE de destino remoto.

4. El dispositivo DTE lee el campo Dirección con el bit de la FECN que se establece en 1.

5. Este parámetro indica que la trama experimentó congestión en la ruta desde el origen hasta el destino.

BECN

La BECN informa al dispositivo de origen que hay congestión en la ruta de la red. El bit de la BECN también forma parte del campo Dirección en el encabezado de la trama de Frame Relay. Una BECN funciona de la siguiente manera:

1. Un switch Frame Relay detecta congestión en la red.

2. Establece el bit de la BECN en 1 en las tramas que se dirigen en dirección opuesta a las tramas que el bit de la FECN marca.

3. Este parámetro le informa al dispositivo DTE de origen que se congestionó una ruta particular a través de la red.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Arrastrar cada definición hasta el término Frame Relay correspondiente y luego haga clic en Verificar.

8.2.4 Creación del prototipo de la WAN

Refiera a la **Figura** del curso en línea

Para configurar el prototipo de la WAN de Frame Relay, el personal de CompañíadeRedes primero configura el router FR1 para que actúe como el switch Frame Relay. El personal utiliza el comando **`frame-relay switching`** para iniciar la configuración. Este comando le ordena al router que funcione como dispositivo DCE y que simule un switch Frame Relay. Los comandos de configuración **`frame-relay route`** adicionales se aplican al router para habilitarlo a que conmute los DLCI de cada interfaz.

Las dos interfaces seriales de FR1 se pueden configurar ahora como los dispositivos DCE de Frame Relay. La encapsulación Frame Relay debe especificarse en cada interfaz. Las dos encapsulaciones Frame Relay posibles son **ietf** y **cisco**. La encapsulación predeterminada es **cisco**. El método **cisco** tiene patente y no debería utilizarse si el router se conecta a un router que no es de Cisco a través de una WAN de Frame Relay.

El diseñador de red configura Frame Relay al configurar la dirección IP de Capa 3 en la interfaz y al establecer el tipo de encapsulación de Frame Relay. La encapsulación se establece mediante este comando:

```
Router(config-if)#encapsulation frame-relay {cisco ¦ ietf}
```

Los routers CPE no necesitan configurarse como switches Frame Relay. Sin embargo, la interfaz serial del router CPE necesita configurarse con la encapsulación Frame Relay y una dirección IP. El diseñador utiliza los nombres de los dispositivos que se planearon y sus direcciones durante la prueba.

En la red prototipo, no hay dispositivo CSU/DSU que proporcione la temporización. Por lo tanto, es importante configurar una frecuencia de reloj en las interfaces seriales de FR1.

Refiera a la **Figura** del curso en línea

Durante el ensayo de prototipo, el router FR1 funciona como el switch Frame Relay en el proveedor de servicio. Esto simula la conectividad a través de la nube Frame Relay. Se crea un circuito virtual entre Margen2 y los routers BR3. Este circuito se comporta de la misma manera que un enlace que se conecta directamente.

ARP inverso y asignaciones Frame Relay

El Protocolo inverso de resolución de dirección (***ARP inverso***) proporciona un mecanismo para crear asignaciones dinámicas de dirección DLCI a Capa 3. El ARP inverso funciona de manera similar a un ARP en una red Ethernet local. Con ARP, el dispositivo emisor conoce la dirección IP de Capa 3. Envía broadcast para conocer la dirección MAC del enlace de datos remoto. Con ARP inverso, el router conoce la dirección de Capa 2, que es el DLCI. Envía solicitudes para la dirección IP de Capa 3 remota.

Cuando una interfaz de un router Cisco se configura para que utilice la encapsulación Frame Relay, el ARP inverso se activa de manera predeterminada. Es posible configurar una asignación estática en forma manual para un DLCI específico. La asignación estática se utiliza si el router en el otro extremo no admite el ARP inverso.

Refiera a la **Figura** del curso en línea

Una ventaja de la conectividad Frame Relay es que una interfaz física puede admitir muchos circuitos virtuales. Frame Relay habilita una conexión a la red de conmutación por paquete del proveedor para proporcionar conectividad a muchos sitios remotos. Este tipo de WAN ***multiacceso*** es menos costosa que una que requiere enlaces punto a punto que se dedican entre los sitios.

Los enlaces múltiples que comparten una única interfaz pueden ocasionar problemas cuando se actualiza el protocolo de enrutamiento vector distancia. Frame Relay es un protocolo multiacceso que no es de broadcast (***NBMA***). Esto significa que cada circuito virtual de una interfaz se trata como una red local por separado. ***Horizonte dividido*** evita que las actualizaciones de la tabla de enrutamiento salgan de la interfaz que las recibe. Gracias a esto, si un sitio remoto envía una actualización de protocolo de enrutamiento, dicha actualización no se envía a los otros circuitos virtuales que comparten la misma interfaz física.

Para evitar los problemas que ocasiona el horizonte dividido, la interfaz física se divide en ***subinterfaces*** lógicas. Los dos tipos de subinterfaces Frame Relay son punto a punto y multipunto.

Punto a punto

En el caso de las subinterfaces punto a punto, se utiliza una única subinterfaz para establecer una conexión de circuito virtual permanente (***PVC***) a otra interfaz física o subinterfaz de un router remoto. Cada par de interfaces se encuentra en su propia subred y cada interfaz tiene un único DLCI. Los broadcast no presentan problemas en este entorno porque los routers se conectan punto a punto y actúan como líneas arrendadas.

Multipunto

En el caso de las subinterfaces multipunto, se utiliza una única subinterfaz para establecer múltiples conexiones PVC a múltiples interfaces físicas o subinterfaces en routers remotos. Esta configuración no resuelve los problemas de horizonte dividido. El horizonte dividido debe desactivarse para que los protocolos de enrutamiento vector distancia funcionen con los enlaces multipunto.

Refiera a la **Figura** del curso en línea

Una vez que se configura la WAN de Frame Relay es necesario verificar que funcione según lo esperado. En el router CPE, hay una cantidad de comandos **`show`** que muestran información sobre el estado del bucle local de Frame Relay y el circuito PVC.

El comando **`show interfaces serial`** muestra el estado de las interfaces y los detalles sobre la encapsulación, DLCI, tipo de LMI y las estadísticas de la LMI. Durante el funcionamiento normal de Frame Relay, el resultado del comando show interface serial debería indicar que la interfaz está activa y que el protocolo de línea está activo.

Para verificar el intercambio de mensajes de LMI entre el router CPE y el switch Frame Relay local, utilice el comando **`show frame-relay lmi`**.

El comando **`show frame-relay pvc`** `[`**`interface`** *`interface`*`]` `[`**`dlci`**`]` muestra el estado de cada PVC que se configura y las estadísticas del tráfico. Este comando además resulta útil para ver la cantidad de paquetes de BECN y FECN que recibe el router.

Utilice el comando **`show frame-relay map`** para mostrar las entradas actuales que se aprendieron mediante el ARP inverso, las asignaciones que se configuran de manera estática y la información acerca de las conexiones.

Para borrar las asignaciones Frame Relay que se crearon en forma dinámica mediante ARP inverso, utilice el comando **`clear frame-relay-inarp`**.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

8.2.5 Diagnóstico de fallas del funcionamiento de Frame Relay

Refiera a la **Figura** del curso en línea

Luego de probar la conectividad Frame Relay básica, el diseñador de red y el personal de CompañíadeRedes deciden probar las capacidades de respaldo. Establecen conexiones Ethernet entre los routers. Estas conexiones Ethernet pretenden simular las VPN existentes entre los sitios remotos y la red principal del estadio. A la topología se agrega otro router, a la que se le denomina ISPX, para simular la conectividad ISP.

Configuración del enlace de respaldo

Se debe configurar el enrutamiento en los dos routers CPE para que se utilice el enlace de respaldo si falla el enlace Frame Relay. Una forma de configurar los routers para que utilicen el respaldo es crear ***rutas estáticas flotantes***.

Una ruta estática flotante es una ruta estática que tiene una distancia administrativa mayor que la distancia administrativa de las rutas dinámicas correspondientes. El personal puede configurar una ruta estática con el uso de las interfaces Fast Ethernet. La configuración especifica una mayor distancia administrativa que la ruta Frame Relay mediante el siguiente comando:

```
Edge2(config)#ip route 172.18.225.0 255.255.255.0 172.18.0.250 130
```

Esta ruta, con una distancia administrativa de 130, sólo se instala en la tabla de enrutamiento si la otra ruta se pierde debido a una falla del enlace o alguna otra causa. De esta forma, mientras la ruta que utiliza la conexión Frame Relay esté disponible, no se utiliza la interfaz Fast Ethernet.

El diseñador crea un plan de prueba para verificar el desempeño de los enlaces de respaldo en caso de producirse una falla.

Refiera a la **Figura** del curso en línea

Resolución de problemas de una falla del enlace principal

En un diseño WAN, el diseñador de red debe garantizar que haya enlaces de respaldo y que funcionen correctamente en caso de que se produzca una falla en el enlace principal. Frame Relay y otras tecnologías WAN son generalmente servicios muy confiables. Sin embargo, a veces la red WAN funciona a niveles menores de lo esperado o el circuito está sin activar. Un enlace de respaldo puede transportar el tráfico en estas circunstancias o cuando se necesita resolver problemas y reparar una falla de la conexión principal.

La resolución de problemas de un circuito Frame Relay es un proceso de varios pasos que abarca la funcionalidad de las Capas 1, 2 y 3.

Control del estado de la interfaz Frame Relay

El primer paso para verificar o resolver problemas de la configuración de Frame Relay es utilizar el comando **`show interface serial`**. Si el resultado del comando **`show interface serial`** indica que tanto la interfaz como el protocolo de línea están sin habilitar, esto generalmente indica un problema en la Capa 1. Puede haber un problema con el cable o la CSU/DSU que debe corregirse.

La interfaz puede también mostrar una condición de inactividad si la configuración estática del DLCI es incorrecta. Para verificarlo, utilice el comando **`show frame-relay pvc`**. El estado **`ELIMINADO`** del PVC puede indicar que el DLCI que se configuró en el dispositivo CPE no coincide con el DLCI que se asignó al circuito.

Verificación del funcionamiento de la LMI

Cuando el resultado de un comando **`show interface serial`** indica que la interfaz está activa, pero el protocolo de línea está inactivo, puede haber un problema en la Capa 2. Es posible que la interfaz serial no esté recibiendo los mensajes de actividad de la LMI desde el switch Frame Relay.

El siguiente paso en la resolución de problemas del circuito Frame Relay es verificar que los mensajes de la LMI se envían y reciben en forma correcta. Utilice el comando **`show frame-relay lmi`** y busque un valor distinto a cero en cualquiera de los contadores **`No válidos`**. Además, asegúrese de que el tipo de LMI sea correcto para el circuito.

Depuración del intercambio LMI

Refiera a la **Figura** del curso en línea

Si el tipo de LMI es correcto para el circuito, pero se indican mensajes no válidos, el comando **`debug frame-relay lmi`** puede proporcionar más información. El resultado del comando **`debug`** muestra los mensajes de la LMI a medida que se envían y se reciben entre el switch Frame Relay y el router CPE en tiempo real.

El resultado (**`salida`**) indica los mensajes de estado de la LMI que envía el router. El resultado (**`entrada`**) indica un mensaje que se recibe del switch Frame Relay.

Un mensaje **`tipo 0`** es un mensaje de estado LMI completo. Dentro del mensaje de estado, el resultado **`dlci 110`**, **`status 0x2`** indica que el **`DLCI 110`** está activo. Los valores comunes del campo de estado del DLCI son:

0x0: Agregado e inactivo. El switch programó este DLCI, pero no puede utilizarse.

0x2: Agregado y activo. El switch Frame Relay tiene el DLCI y todo está en funcionamiento.

0x4: Eliminado. El switch Frame Relay no programó DLCI para el router. Este estado puede darse si se invierten los DLCI en el router o si se borró el PVC en la nube Frame Relay.

Un mensaje **`tipo 1`** indica un intercambio de actividad de LMI.

Control de la funcionalidad de Capa 3

A veces, las funciones de Capa 1 y 2 están activas, pero no hay comunicación IP sobre el PVC. Para que un router llegue a un router remoto a través de la red Frame Relay, debe asignar la dirección IP del router remoto con el DLCI local correcto. Si la dirección IP del router remoto no aparece en la tabla de asignación Frame Relay, es posible que no admita el ARP inverso. Es posible que se requiera la configuración de la dirección IP hacia la asignación del DLCI mediante el comando **`frame-relay map ip`** `{`*`ip address`*`}{`*`dlci`*`} [`**`broadcast`**`]`.

Además, es necesario verificar que tampoco existen listas de control de acceso o problemas con la tabla de enrutamiento IP. Aunque estos tipos de problemas no se relacionen directamente con el funcionamiento del circuito WAN, pueden sugerir que el circuito no funciona correctamente.

Actividad de Packet Tracer

Refiera a la actividad de "**Packet Tracer**" del curso en línea

Cuando utilice el plan de prueba y la red prototipo, configure los enlaces de respaldo y verifique que la conmutación por error funcione según se espera.

Se debería descargar este documento para realizar la actividad de Packet Tracer:

1. Plan de prueba de redundancia del estadio

Actividad en el laboratorio

Refiera a la **actividad de laboratorio** del curso en línea

Cuando utilice el plan de prueba y la red prototipo de CompañíaCinematográfica, configure los enlaces de respaldo y verifique que la conmutación por error funcione según se espera.

8.2.6 Identificación de riesgos y debilidades

Refiera a la **Figura** del curso en línea

Luego de finalizar la prueba prototipo de la WAN, el diseñador de red y el personal de CompañíadeRedes analizan los resultados de la prueba. La configuración de Frame Relay funciona

según lo esperado y los enlaces de respaldo protegen la conectividad WAN en caso de que falle el enlace Frame Relay.

Sin embargo, existen algunos riesgos que se relacionan con la configuración de Frame Relay que deben comunicarse a la administración del estadio.

Áreas de riesgo

El área de riesgo más crítica es el desempeño de los enlaces de la VPN ya que deben funcionar correctamente cuando se utilizan como respaldos. Cuando los componentes de voz y video de la red se agregan al tráfico WAN existente, puede ocasionar un problema con la calidad del servicio si se debe utilizar la conexión de la VPN. La VPN actual a través del ISP no tiene un nivel de servicio que se garantice. Además, no tiene mecanismos para proporcionar la calidad de servicio. Como resultado, los enlaces de respaldo sólo pueden proporcionar conectividad limitada en caso de falla.

No es posible probar el desempeño a través de la red Frame Relay del TSP actual; por lo tanto, existe un riesgo que se asocia con el diseño. La aceptación final del diseño no puede realizarse hasta que se conozcan los resultados de la instalación piloto.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Analice los resultados de la prueba prototipo de CompañíaCinematográfica y documente todos los riesgos o debilidades del diseño. Complete la sección Conclusiones del plan de prueba.

8.3 Creación de un prototipo para el soporte del trabajador remoto

8.3.1 Identificación de los requisitos y objetivos de la VPN

Refiera a la **Figura** del curso en línea

Un objetivo comercial de alta prioridad del diseño de la red del estadio es ofrecer servicios adicionales a los clientes y proveedores del estadio para mejorar la experiencia del estadio.

Requisitos de la oficina del equipo

Las oficinas del equipo solicitan un método seguro para que sus miembros se conecten a los servidores del equipo. Los exploradores necesitan transmitir información sobre posibles clientes a los servidores del equipo cuando no estén en el estadio. Debido a que esta información es sumamente confidencial, el equipo quiere que los exploradores puedan conectarse en forma remota a través de la VPN. Una VPN es una extensión de la red privada interna. Las VPN transmiten información en forma segura a través de redes públicas o compartidas, tales como Internet. El diseñador de red necesita considerar el impacto de la red al proporcionar este servicio.

Cómo funciona una VPN

Una VPN emula un enlace punto a punto. La VPN encapsula los datos con un encabezado que proporciona la información de enrutamiento. Este formato permite que los datos atraviesen la red pública y lleguen a su destino. Para emular un enlace privado, los datos encapsulados se encriptan para mantener su confidencialidad. Los algoritmos de encriptación garantizan que si se interceptan los paquetes en la red pública, no podrán leerse sin las claves de encriptación.

Los exploradores del equipo, así como otros miembros que trabajan desde sus hogares o mientras viajan, pueden utilizar las conexiones de la VPN para acceder de manera remota a los servidores que se ubican en el estadio. Desde la perspectiva de los usuarios, la VPN es una conexión punto a punto entre la computadora (el cliente de la VPN) y un extremo de la VPN (el servidor de la VPN o su concentrador) en el estadio.

Refiera a la **Figura** del curso en línea

Se corre riesgo cuando se extiende la LAN privada para incluir a trabajadores remotos.

Seguridad de la VPN

En muchas empresas, se considera que los trabajadores remotos que acceden a recursos en el sitio central a través de una VPN son usuarios "confiables", al igual que aquellos trabajadores que realmente trabajan en el lugar. A diferencia de los trabajadores del lugar, los usuarios de la VPN pueden acceder a la red desde dispositivos que no son completamente seguros o desde ubicaciones no seguras en áreas públicas. Se necesita tener sumo cuidado para garantizar que estos trabajadores remotos no tengan acceso a recursos o áreas de la red que no necesitan para realizar su trabajo.

Ubicación del servidor de la VPN

El diseñador de red sabe que los datos encriptados no pueden filtrarse hasta que se descifren en el extremo del servidor de la VPN. Por este motivo, la ubicación del servidor de la VPN en la red es muy importante. Debe ubicarse en un punto donde los paquetes entrantes puedan analizarse y filtrarse antes de entregarse a los recursos de red internos.

8.3.2 Creación del plan de prueba

¿Qué necesita probarse?

Refiera a la **Figura** del curso en línea

El estadio utiliza las redes VPN para conectarse a la tienda de recuerdos y a los centros de venta de entradas. Estas VPN son VPN de sitio a sitio que administra el ISP y no necesitan someterse a prueba.

Soporte a los exploradores del equipo

Para los clientes remotos, existen dos opciones disponibles para respaldar los requisitos de la VPN de los exploradores del equipo:

- ***Opción 1:*** La administración del estadio puede solicitar servicios de VPN adicionales del ISP actual.
- ***Opción 2:*** El servidor de la VPN puede instalarse en la red del estadio.

Administración del servidor de la VPN

El diseñador sugiere utilizar tunneling dividido para permitir que los usuarios envíen el tráfico que se destina a la red corporativa a través del túnel de la VPN mientras que todo el otro tráfico se envía hacia Internet a través de la LAN local del cliente VPN. El diseñador debe determinar si el personal actual del estadio puede configurar y administrar un servidor de la VPN. Para hacerlo, el diseñador decide probar la facilidad para configurar e instalar el servidor de la VPN y el software del cliente. Luego de configurar la VPN, el diseñador prueba las ACL para filtrar el tráfico proveniente de la VPN y la ubicación del servidor de la VPN en la red.

Cisco EasyVPN

El diseñador decide que Cisco EasyVPN es la mejor opción para configurar y administrar la conectividad del usuario remoto a la VPN. La EasyVPN es una herramienta del software IOS de Cisco. Facilita la configuración de un router o artefacto de seguridad Cisco como un extremo o servidor de la VPN.

Para el prototipo, el diseñador selecciona la función Seguridad Avanzada IP que se establece para el router 1841. La interfaz ***SDM*** de Cisco para el 1841 puede utilizarse para configurar el servidor EasyVPN para los clientes remotos.

Refiera a la **Figura** del curso en línea

La solución Cisco EasyVPN

Es importante que la implementación sea fácil para asegurar que la VPN puede respaldar a los exploradores del equipo móvil. Cisco EasyVPN consta de dos componentes:

- **Servidor Cisco EasyVPN**: este servidor puede ser un router o un gateway dedicado de la VPN, tal como un firewall PIX o un concentrador de VPN. Un gateway de VPN que utiliza el software del servidor Cisco EasyVPN puede finalizar las VPN de acceso remoto y las conexiones VPN de sitio a sitio.
- **Cisco EasyVPN remota**: Cisco EasyVPN remota permite que los dispositivos remotos reciban las políticas de seguridad de un servidor Cisco EasyVPN. Esto minimiza los requisitos de configuración en la ubicación de la VPN remota. Cisco EasyVPN remota permite que los parámetros de la VPN se envíen desde el servidor hasta el dispositivo remoto. Los parámetros de la VPN incluyen las direcciones IP internas, las máscaras de subred internas y las direcciones del servidor de DHCP.

El diseñador de red crea un plan de prueba para verificar el uso de Cisco EasyVPN para configurar un servidor de la VPN para el estadio y para configurar el software del cliente.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un plan de prueba para configurar y probar una configuración del cliente VPN para CompañíaCinematográfica.

Se debería descargar este documento para realizar la actividad en el laboratorio:

1. Plan de prueba del diseño de la VPN

8.3.3 Validación de la opción de topología de la VPN, dispositivos y topologías

Refiera a la **Figura** del curso en línea

Antes de probar la configuración del prototipo de la VPN, el diseñador de red necesita tener en cuenta a varios protocolos, algoritmos y opciones.

Componentes de la VPN

Las VPN tienen dos componentes importantes:

- Tunneling para crear la red virtual
- Encriptación para habilitar la privacidad y la seguridad

Red virtual

Para construir una red virtual, se crea un ***túnel*** entre los dos extremos. En una ***VPN de sitio a sitio***, los host envían y reciben tráfico TCP/IP normal a través de un gateway de la VPN. Un gateway puede ser un router, firewall, ***concentrador de VPN*** o artefacto de seguridad. El gateway se ocupa de encapsular el tráfico saliente de un sitio y de enviarlo por un túnel a través de una red hacia un gateway peer en el sitio remoto. Es posible que un túnel no pueda garantizar la seguridad. El túnel simplemente crea una extensión de la red local a través de la WAN o de la red pública. Los túneles pueden trasladar contenido con o sin encriptar. Cuando lo recibe, el gateway peer remoto elimina los encabezados, descifra el paquete y lo transmite hacia el host de destino de su red privada. En una ***VPN de acceso remoto***, el cliente VPN de la computadora del usuario hace contacto con el gateway para establecer el túnel.

Protocolos VPN Tunnel Protocols

Los túneles de la VPN se crean mediante el uso de varios protocolos de encapsulación diferentes. Estos protocolos incluyen:

- Encapsulación de enrutamiento genérico (***GRE***)
- Seguridad IP (***IPSec***)
- ***Protocolo L2F***
- Point-to-Point Tunneling Protocol (***PPTP***)
- Layer 2 Tunneling Protocol (***L2TP***)

Refiera a la **Figura** del curso en línea

No todos los protocolos ofrecen el mismo nivel de seguridad.

Las tecnologías VPN utilizan algoritmos de encriptación que previenen que los datos se lean si se interceptan. Un algoritmo de encriptación es una función matemática que combina el mensaje con una cadena de dígitos a la que se le denomina clave. El resultado es una ***cadena de cifrado*** ilegible. El descifrado es extremadamente difícil o imposible sin la clave correcta. Los métodos de encriptación más comunes que se utilizan para las VPN son el estándar de encriptación de datos (***DES***), el DES triple (***3DES***), el estándar de encriptación avanzada (***AES***) y Rivest, Shamir y Adleman (***RSA***).

Algoritmos de encriptación

Los algoritmos de encriptación, tales como DES y 3DES, requieren una clave secreta simétrica y compartida para llevar a cabo la encriptación y el descifrado. El administrador de red puede configurar las claves en forma manual.

Otra posibilidad es configurar las claves mediante el uso de un método de intercambio de claves. El acuerdo de claves Diffie-Hellman (***DH***) es un método de intercambio de claves público. Ayuda a que dos peers establezcan una clave secreta compartida, que sólo ellos conocen, mientras se comunican a través de un canal sin protección. Los grupos Diffie-Hellman especifican el tipo de ***criptografía*** que se utilizará:

- **GRUPO DH 1**: utiliza una criptografía de 768 bit.
- **GRUPO DH 2**: IOS de Cisco, firewall PIX y dispositivos de seguridad adaptables (ASA) de Cisco solamente. Especifica el uso de criptografía de 1024 bit.
- **GRUPO DH 5**: se admite si se cumplen los requisitos del sistema del software. Especifica el uso de criptografía de 1536 bit.

Refiera a la **Figura** del curso en línea

Para proteger contra la intercepción y modificación de los datos de la VPN, se puede utilizar un algoritmo de ***integridad de datos***. Un algoritmo de integridad de datos agrega un ***hash*** al mensaje. Si el hash transmitido coincide con el hash recibido, el mensaje recibido se acepta como una copia exacta del mensaje transmitido. El código de autenticación de mensajes que se basa en funciones hash criptográficas (***HMAC***) es un algoritmo de integridad de datos que garantiza la integridad del mensaje. Hay dos algoritmos HMAC comunes:

- HMAC-Message Digest 5 (***MD5***): este algoritmo utiliza una clave secreta compartida de 128 bit. El mensaje de longitud variable y la clave secreta compartida de 128 bit se combinan y ejecutan a través del algoritmo hash HMAC-MD5. El resultado es un hash de 128 bit. El hash se adjunta al mensaje original y se envía al extremo remoto.
- HMAC-Algoritmo de hash seguro 1 (***HMAC-SHA-1***): este algoritmo utiliza una clave secreta de 160 bit. El mensaje de longitud variable y la clave secreta compartida de 160 bit se

combinan y ejecutan a través del algoritmo de hash HMAC-SHA-1. El resultado es un hash de 160 bit. El hash se adjunta al mensaje original y se envía al extremo remoto.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Complete el crucigrama de acuerdo con la información sobre VPN que se analizó.

8.3.4 Prototipo de la conectividad de la VPN para trabajadores remotos

Refiera a la **Figura** del curso en línea

En la red propuesta para el estadio, el diseñador de red selecciona la tecnología IPSec para las VPN de acceso remoto.

IPSec

IPSec es un marco de estándares abiertos. Proporciona confidencialidad, integridad y autenticación de datos entre los pares que participan. IPSec proporciona estos servicios de seguridad en la Capa 3.

IPSec confía en los algoritmos existentes para implementar la encriptación, la autenticación y el intercambio de claves. Cuando se configura el servidor de la VPN, se deben configurar los siguientes parámetros:

- **Un protocolo IPSec**: las opciones son la carga útil de seguridad encapsulada (***ESP***), el encabezado de autenticación (***AH***), o ESP con AH.
- **Un algoritmo de encriptación que sea apropiado para el nivel de seguridad deseado**: las opciones son DES, 3DES o AES.
- **Un algoritmo de autenticación para proporcionar la integridad de los datos**: las opciones son MD5 o SHA.
- **Un grupo Diffie-Hellman**: las opciones son DH1, DH2 y DH5, si se admiten.

IPSec puede utilizar el intercambio de claves por Internet (***IKE***) para manejar la negociación de protocolos y algoritmos. El IKE también puede generar las claves de autenticación y encriptación que utiliza IPSec.

Refiera a la **Figura** del curso en línea

Los clientes VPN reciben una interfaz de red lógica con una dirección IPv4 que es importante en la red interna del sitio central. Esta dirección IPv4 generalmente proviene de un rango de dirección IP privada. Como resultado, es posible que los usuarios de la VPN no puedan acceder a sus recursos locales, tales como impresoras y servidores.

Split tunnel

En una situación común de cliente VPN, todo el tráfico proveniente del cliente VPN se encripta mediante la interfaz de red lógica. Luego se envía al servidor de la VPN, independientemente del destino del tráfico. El ***Tunneling dividido*** permite a los usuarios enviar sólo el tráfico que se destina a la red corporativa a través del túnel. El tráfico restante se envía a Internet a través de la LAN local del cliente VPN. Los ejemplos del otro tráfico son la mensajería instantánea, el correo electrónico y la exploración Web informal. El software del cliente VPN de Cisco puede configurarse para split tunnel mediante la habilitación de la opción de acceso a la LAN local. El tunneling dividido aumenta los riesgos de seguridad porque un ataque contra la red protegida puede venir desde el Internet del cliente.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Explore las opciones de configuración para crear un servidor Cisco EasyVPN mediante el uso del SDM de Cisco.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Mediante el plan de prueba, configure y realice la prueba del cliente VPN.

8.3.5 Validación de la ubicación del servidor de la VPN

Refiera a la **Figura** del curso en línea

El diseñador de red debe decidir dónde ubicar el servidor de la VPN antes de determinar cómo y dónde filtrar y controlar el tráfico.

Ubicación del servidor de la VPN

Los servidores de la VPN suelen ubicarse en el extremo WAN de una red. En estos casos, se utilizan los firewall o las ACL para garantizar que los usuarios de la VPN tengan acceso sólo a los recursos de red apropiados.

Si la administración del estadio opta por instalar un servidor de VPN local, el diseñador recomienda ubicar el servidor de VPN en el mismo dispositivo que proporciona el filtrado de firewall para los servidores. El tráfico de usuario remoto puede descifrarse y filtrarse antes de que se envíe al servidor.

El diseñador crea una topología de prueba que es similar a la topología que se utiliza en la prueba del prototipo del conjunto de servidores. El diseñador crea entonces una lista de verificación para la instalación y un plan de prueba para comprobar el funcionamiento de la VPN y el filtrado de la ACL.

8.3.6 Identificación de riesgos o debilidades

Refiera a la **Figura** del curso en línea

Una vez que se finalice la prueba, el diseñador de red analiza los resultados para determinar el nivel de riesgo en el diseño.

Riesgos en el diseño de la VPN

En el diseño de la VPN que admite el personal del equipo remoto, el riesgo principal se relaciona con la capacidad que tiene el personal de soporte de TI existente para configurar y mantener el servidor de la VPN. También es riesgoso configurar clientes a medida que se necesite.

Parece que el uso de SDM y Cisco EasyVPN es la opción correcta para configurar y mantener la VPN de acceso remoto para la red del estadio. Suele ser relativamente fácil crear una conectividad segura para los trabajadores remotos.

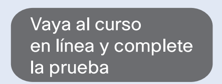
Una vez que finalice la totalidad de la prueba piloto, el diseñador puede trabajar con el resto del personal de CompañíadeRedes para preparar la presentación del diseño final para la actualización de la red del estadio.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

Determine si cada sigla representa un término de tunnelling o un término de encriptación. Arrastre cada término hasta la categoría de seguridad correcta y luego haga clic en Verificar.

Resumen del capítulo



Examen del capítulo

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 9

Preparación de la propuesta

Introducción

Refiera a la **Figura** del curso en línea

9.1 Recopilación de la información existente para la propuesta

9.1.1 Organización de la información existente

Refiera a la **Figura** del curso en línea

Después de probar el diseño de red propuesto, el diseñador de red recopila la información que ha reunido de la solicitud de propuesta (RFP) y los pasos previos del proceso PPDIOO (Preparar, Planificar, Diseñar, Implementar, Operar, Optimizar) en una propuesta de red. Generalmente, la propuesta contiene las siguientes secciones:

- Resumen ejecutivo
- Requisitos de la red
- Entorno de la red actual
- Diseño físico propuesto
- Diseño lógico propuesto
- Plan de implementación
- Cálculo de los costos

Si la propuesta responde a una RFP, los componentes de la propuesta y el índice se ensamblan siguiendo estrictamente el formato solicitado en la RFP.

Si no hay una RFP escrita o si la RFP escrita no especifica un bosquejo o formato, el diseñador puede determinar el esquema y diseño de la propuesta. En estos casos, el diseño de la propuesta debe ser fácil de leer y ayudar al lector a encontrar la información. Los gráficos mejoran la legibilidad de una propuesta y además transmiten información. El texto debe ser legible, generalmente con fuentes tipo serif como Times Roman de entre 10 y 12 puntos. Los márgenes de la página deben ser por lo menos de 0.5 pulgadas y los números de página deben estar incluidos en la parte superior o en la parte inferior de cada página.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de pantalla completa

9.1.2 Integración de la información existente

Refiera a la **Figura** del curso en línea

En esta etapa del proyecto del estadio, el gerente de cuentas y el diseñador de red de la CompañíadeRedes elaboran una propuesta como respuesta a la RFP de CompañíaEstadio. La mayor parte del material de origen de la propuesta ya está disponible, excepto el plan de implementación y el cálculo de los costos.

Antes de desarrollar el plan de implementación y el cálculo de los costos, el diseñador edita y organiza la información existente.

Resumen ejecutivo

Por lo general, el gerente de cuentas asignado a la cuenta del cliente se encarga de elaborar el Resumen ejecutivo. El informe se redacta desde la perspectiva del cliente y hace hincapié en los beneficios que generará la red propuesta para la organización del cliente. Los objetivos del proyecto previamente identificados y priorizados, así como la información del alcance del proyecto, constituyen la base del Resumen ejecutivo.

Requisitos de la red y entorno de la red actual

Estas secciones contienen la información del documento Requisitos de diseño creado y aprobado anteriormente en el proceso PPDIOO. La información se incluye de manera que el cliente pueda verificar que el diseño propuesto reúne los requisitos acordados.

Diseño físico y lógico

El diseñador elabora las secciones del diseño físico y lógico propuesto a partir de los diagramas de diseño propuestos y los resultados del prototipo y la prueba piloto. Es importante incluir en esta sección todos los riesgos identificados y las estrategias para mitigarlos. Esta información ayuda al cliente a tomar decisiones informadas respecto a los diferentes elementos del diseño.

Refiera a la **Figura** del curso en línea

Durante el proceso de ensamblado de la propuesta, el diseñador de red y el gerente de cuentas revisan todo el material para asegurarse de que esté completo. Es importante que la administración de la CompañíaEstadio y el personal técnico puedan encontrar y comprender fácilmente el material incluido en la propuesta. Una propuesta desorganizada o incompleta puede hacer que el cliente contrate a otra persona para realizar el proyecto.

El diseñador y el gerente de cuentas trabajan juntos para completar la planificación de la implementación y para crear la propuesta de costos.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Prepare un bosquejo de una propuesta de red para la CompañíaCinematográfica.

9.2 Desarrollo del plan de implementación

9.2.1 El plan de implementación

Refiera a la **Figura** del curso en línea

En el proceso PPDIOO, el siguiente paso después de terminar el diseño de la red es desarrollar el plan de implementación y de migración. Es fundamental que se incluya la mayor cantidad posible de detalles para los ingenieros y los técnicos de red.

Implementación del diseño de red

La implementación de un diseño de red implica instalar hardware, configurar sistemas, probar la red y poner la red en producción. Cada tarea consiste en varios pasos. Cada tarea requiere además la siguiente documentación:

- Una descripción de la tarea
- Referencias a los documentos de diseño
- Guía detallada para la implementación

- Guía detallada de restitución (rollback) en caso de falla
- El tiempo necesario estimado para la implementación

Diseño del estadio

Se identificaron los criterios de éxito y fracaso para todos los aspectos del diseño de red del estadio y se integraron a la documentación de diseño.

Cuando el diseñador de red implementa un diseño, debe considerar un posible fracaso aun después de una prueba piloto o una prueba de prototipo de red exitosa. Es posible que sea necesario realizar otras pruebas en cada paso de la implementación para asegurarse de que la red funciona tal como ha sido diseñada.

Refiera a la **Figura** del curso en línea

Aprobación del cliente

El plan de implementación del estadio detalla las tareas necesarias para alcanzar los objetivos del proyecto. El plan incluye las expectativas del cliente y los criterios para el éxito, que el cliente debe aprobar y firmar para iniciar el proyecto.

Tan pronto como se obtiene la aprobación del cliente al plan de implementación, puede comenzar la instalación.

El cliente recibe una lista detallada de todos los dispositivos necesarios y de las tareas que se llevarán a cabo. Esta lista forma parte del plan de implementación. El diseñador de red y el gerente de cuentas conservan una copia firmada de esta lista.

A medida que se completa cada tarea, el cliente debe firmar ratificando que la tarea se ha completado y que los resultados son los esperados.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad de pantalla completa

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un plan de implementación para la instalación de la CompañíaCinematográfica.

9.2.2 Definición del mejor método de instalación

Refiera a la **Figura** del curso en línea

Existen tres métodos de instalación que se pueden utilizar para la implementación.

- ***Nueva instalación:*** comúnmente conocida como una *instalación en terreno no explotado (greenfield)*
- ***Instalación en fases:*** se instalan componentes en una red existente que se encuentra en funcionamiento
- ***Reemplazo total:*** comúnmente conocido como (fork-lift upgrade) *actualización de gran escala*

Nueva instalación

En una instalación nueva, no hay usuarios actuales o aplicaciones que se ejecuten actualmente. Esta situación brinda muchas ventajas:

- Se pueden instalar y probar todos los equipos y servicios al mismo tiempo.
- El plan de implementación de una red nueva no es tan complejo como los otros dos tipos de instalación.
- Los programas son más flexibles que en los casos que ya existe una red.
- Las interrupciones para la compañía son mínimas.

Instalación en fases en una red existente

En una instalación en fases, las partes de la actualización de la red se implementan de forma separada respecto a las partes actualmente en ejecución.

Cuando se instalan nuevos componentes o nuevas tecnologías de red en una red existente, se debe tener mucho cuidado de no interrumpir los servicios innecesariamente. Una implementación en fases requiere una planificación más detallada con el cliente. La actualización de la red se divide en partes más pequeñas que se pueden instalar y probar rápidamente. La instalación de la actualización en fases más pequeñas genera un tiempo mínimo de inactividad.

Refiera a la **Figura** del curso en línea

La desventaja de este método es que posiblemente requiera más tiempo y fondos para completarse.

Reemplazo total de la red

A veces no es necesario reemplazar por completo una red actual. El reemplazo total de la red generalmente tiene lugar cuando la red es obsoleta y no se puede actualizar. En esta situación, por lo común se construye la red nueva en forma paralela a la red actual. Cuando la red nueva funciona, puede haber un periodo para probar esta red en forma paralela con la red anterior. Se establece una fecha para cambiar a la red nueva y luego se desmonta la red anterior.

Método de instalación del estadio

La determinación del mejor método de instalación comienza al inicio de la fase de diseño de la red. El diseñador de red recopila y evalúa la información sobre los objetivos comerciales, los requisitos técnicos y las limitaciones en el diseño.

Dos de los requisitos de la CompañíaEstadio surgen como los factores principales que afectan al método de instalación:

- Los servicios de red del estadio deben estar disponibles durante la actualización.
- Se debe usar el equipo existente en el nuevo diseño de red.

En consecuencia, el diseñador de la CompañíadeRedes recomienda un método de instalación en fases.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un plan con un método de instalación en fases para la CompañíaCinematográfica.

9.2.3 Estimación de programas y recursos

Refiera a la **Figura** del curso en línea

La duración del proyecto es parte del acuerdo contractual. Para cumplir con los plazos del cliente, el diseñador de red crea una programa del proyecto. Tanto la disponibilidad de los materiales como el programa del contratista y el programa del cliente afectan la fecha de inicio y la fecha de finalización.

Cuando el diseñador de red crea un programa del proyecto, debe tener en cuenta la posibilidad de que el proyecto no comience en la fecha de inicio propuesta.

La RFP del estadio indica que el proyecto se debe terminar cuando ambos equipos están fuera de la temporada. Este requisito concede cuatro meses para el programa del proyecto.

Recursos de la CompañíadeRedes

De acuerdo con los conjuntos de tareas requeridos, el diseñador calcula cuáles son los recursos necesarios para implementar la red. Para cumplir con el plazo de 4 meses, la CompañíadeRedes quizá deba aumentar la cantidad de técnicos asignados al proyecto. Posiblemente también sea necesario ajustar la secuencia de tareas para cumplir con la entrega de piezas de equipo específicas o la disponibilidad de los servicios TSP.

Refiera a la **Figura** del curso en línea

Programa estimado

Al desarrollar el programa del proyecto, el diseñador de red considera varios factores:

- Pedido y entrega de los equipos
- Instalación del servicio, como los enlaces WAN
- Programa del cliente, incluidos el mantenimiento disponible y los periodos de inactividad
- Disponibilidad del personal técnico adecuado

Demoras provocadas por el cliente

Con frecuencia, los clientes realizan cambios durante la instalación de un proyecto. Cuando se presentan cambios, el proveedor utiliza el programa para realizar los ajustes en el personal y los demás recursos disponibles.

El diseñador de red también puede usar la documentación del programa para mostrarle a un cliente de qué manera influyen las demoras en la fecha de finalización del proyecto.

Software de gestión de proyectos

Para crear un programa de proyecto, se pueden utilizar herramientas de gestión de proyectos.

Un programa de software puede ser útil para:

- controlar el progreso del proyecto
- mantener el proyecto dentro del programa
- identificar hitos
- realizar el seguimiento de las asignaciones y los costos de las tareas
- advertir al diseñador si el proyecto se retrasa.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un programa para la instalación de la red de la CompañíaCinematográfica.

9.2.4 Planificación de periodos de mantenimiento e inactividad

Periodos de mantenimiento e inactividad

Refiera a la **Figura** del curso en línea

Los periodos de mantenimiento y la inactividad planificada deben estar incluidos en el programa de instalación. Si sólo se dispone de algunas horas al día para hacer cambios en la red, esta limitación se debe reflejar en el programa del proyecto. De lo contrario, los cálculos de tiempo no son exactos y el proyecto puede retrasarse. La programación de la inactividad de la red debe planificarse cuidadosamente para evitar que el cliente sufra serios inconvenientes.

A veces no es posible terminar todas las tareas necesarias durante un periodo de mantenimiento aprobado. Si para una tarea de instalación se requiere que la red, o parte de la red, esté inactiva durante el horario de trabajo normal, es importante contar con el permiso del cliente. Tan pronto como se determine y apruebe el periodo de tiempo, se debe notificar a todas las personas involucradas como corresponde.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear un programa de mantenimiento para la instalación de red de la CompañíaCinematográfica.

9.3 Planificación de la instalación

9.3.1 Creación de la Lista de materiales

Refiera a la **Figura** del curso en línea

Una de las secciones más importantes de la propuesta realizada a la administración del estadio es el cálculo de los costos.

Para preparar el cálculo de los costos, el diseñador de red crea una Lista de materiales (***BOM***). Una BOM es un documento que detalla todo el hardware requerido y los componentes necesarios para implementar la actualización propuesta. Consiste en una lista en la que se enumeran el hardware, el software y los demás elementos que se deben pedir e instalar. El diseñador utiliza esta lista para obtener cotizaciones y hacer los pedidos de equipos.

Pedido de piezas

El diseñador utiliza la BOM para pedir equipos nuevos y repuestos para los equipos existentes. Por lo tanto, cada elemento necesario debe estar incluido en esta lista. Por ejemplo, algunos routers y switches no vienen con soportes de montaje. Estos soportes se deben comprar por separado. Si esta información no está incluida en la BOM, los soportes de montaje pueden quedar fuera del pedido y demorar la instalación del dispositivo.

Refiera a la **Figura** del curso en línea

Para crear la BOM, el diseñador de red examina cada sección de la red para determinar qué piezas del equipo de red se necesitan y las capacidades necesarias en cada dispositivo. Dentro del estadio donde se instalarán o actualizarán los equipos de red, hay 21 ubicaciones separadas:

- 16 armarios de cableado
- 4 ubicaciones de WAN
- 1 centro de datos nuevo

Además, el diseño inalámbrico muestra 33 ubicaciones para la instalación de AP.

Identificación de dispositivos adicionales

Al observar cada área de la red por separado, el diseñador puede identificar fácilmente todos los dispositivos adicionales que sean necesarios. La lista de nuevos equipos requeridos incluye:

- 6 switches de la capa de distribución
- 2 switches de la capa núcleo
- 1 router para la conectividad WAN
- 4 routers para sitios WAN
- 2 controladores de LAN inalámbrica
- 33 AP livianos

Al tomar una decisión con respecto al equipo nuevo, el diseñador debe tener en cuenta el presupuesto en todo momento. El diseñador repasa las opciones de equipos junto con el gerente de cuentas asignado a la cuenta del estadio. Esta colaboración garantiza que los modelos de equipos seleccionados se encuentren dentro de los límites del presupuesto del estadio y que cumplan con los objetivos comerciales actuales y futuros.

Actualizaciones en los dispositivos existentes

Los switches Cisco Catalyst 2960 existentes están incorporados al diseño propuesto. Cada uno de los 16 armarios para cableado contiene uno de estos switches. Los switches 2960 requieren conectividad de fibra redundante para los dispositivos de la capa de distribución. Para agregar

conexiones redundantes, es necesario comprar un transceptor de fibra adicional para cada switch. Estos 16 transceptores adicionales deben estar enumerados en la BOM e incluidos en la propuesta.

Refiera a la **Figura** del curso en línea

Requisitos de software

Durante las primeras etapas de la fase de diseño del estadio, el cliente le entregó al diseñador de red una lista de aplicaciones instaladas actualmente. A partir de esta información y de la auditoría de la red, el diseñador puede identificar todas las aplicaciones existentes.

Aplicaciones existentes

La lista de aplicaciones actuales incluye:

- **Aplicaciones de red**: uso compartido de archivos de Microsoft, impresión, DNS, servidor Web, software de escaneo y reconocimiento
- **Aplicaciones especializadas**: software de escaneo y reconocimiento de entradas
- **Aplicaciones de negocios**: contabilidad, nómina, programación de eventos, gestión de alquileres, mercadotecnia y software de administración de la relación con los clientes (***CRM***)

Nuevas aplicaciones

Entre las aplicaciones nuevas se incluyen:

- **Aplicaciones de red**: software de administración de red
- **Aplicaciones especializadas**: impresión de entradas, cámaras de seguridad y estaciones de visualización IP, sitio de comercio electrónico para la compra de entradas y venta de recuerdos

Las aplicaciones nuevas, los costos de instalación y la capacitación necesaria se agregan a la BOM junto con el hardware identificado. El diseñador contempla si es necesario comprar licencias adicionales para las aplicaciones de software existentes para la actualización de la red.

9.3.2 Recomendación de Servicios SMARTnet

Garantías

Refiera a la **Figura** del curso en línea

Todos los equipos nuevos vienen automáticamente con una ***garantía*** que cubre el dispositivo. Una garantía estándar proporciona los siguientes beneficios:

- ***Hardware:*** garantiza que el hardware no tiene defectos de material o manufactura en condiciones normales de uso.
- ***Software:*** garantiza que los medios físicos no tienen defectos y que el software se ejecuta según las especificaciones publicadas.

Sin embargo, las garantías son limitadas en cuanto a la duración y los servicios que proporcionan. Por ejemplo, una garantía de software normalmente garantiza que el software se ajusta a las especificaciones publicadas para el producto. Se vende explícitamente "como está" y no incluye ninguna versión nueva del software. La mayoría de las garantías se limitan al reemplazo del producto defectuoso y no incluyen soporte técnico o en el lugar.

Contratos de servicio adicional

La red propuesta del estadio incluye la combinación de equipos de red nuevos y otros más viejos. Es probable que las garantías para algunos equipos más antiguos hayan caducado. Para proteger la inversión de EstadioCompañía y para prolongar la vida de los equipos existentes, el gerente de cuentas de CompañíadeRedes recomienda que la administración del estadio compre contratos adicionales de mantenimiento y soporte.

Refiera a la **Figura** del curso en línea

Contratos SMARTnet

El programa SMARTnet es parte de un conjunto de servicios que brindan los Servicios de soporte técnico técnica de Cisco. El programa SMARTnet ofrece al cliente los recursos de soporte para mejoras del servicio y mantenimiento durante la vigencia del contrato.

Un contrato SMARTnet incluye:

- Soporte de software para el software del sistema operativo bajo licencia
- Acceso al Centro de soporte técnico de Cisco (TAC) las 24 horas del día, los 7 días de la semana
- Acceso registrado a Cisco.com para el fácil acceso a la información técnica y la administración de solicitudes de servicio en línea
- ***Reemplazo avanzado*** de piezas de hardware

Tiempos para el reemplazo de hardware

Según el contrato SMARTnet, los tiempos de reemplazo de hardware pueden variar según la urgencia de la necesidad del cliente y la cobertura seleccionada. Por ejemplo, con un contrato de servicio continuo en menos de 2 horas, las 24 horas, todos los días de la semana, los repuestos se entregan dentro de las dos horas siguientes a la determinación de necesidad de una pieza. Este contrato de reemplazo en 2 horas se aplica cualquier día y a cualquier hora de la semana.

Beneficios

El gerente de cuentas de la CompañíadeRedes prepara un cuadro en el que compara los distintos contratos SMARTnet con la garantía básica. Esta comparación se incluye en la propuesta para mostrarle los beneficios al cliente.

Refiera al **Gráfico Interactivo** del curso en línea

Actividad en pantalla completa

9.3.3 Servicios y soporte técnico de Cisco

Refiera a la **Figura** del curso en línea

La actualización de la red del estadio no debe requerir un aumento de la cantidad de personal de soporte de IT. El gerente de cuentas y el diseñador de red de la CompañíadeRedes acuerdan que se deben presentar a la administración del estadio las opciones de asistencia externa.

Servicios de soporte técnico centrada en Cisco

Los servicios de soporte técnico centrada en Cisco consisten en tres niveles de cobertura que brindan al cliente una variedad de opciones.

El gerente de cuentas de la CompañíadeRedes incluye información acerca del contrato del Nivel 2, Servicio de soporte técnico de alto contacto de Cisco en combinación con los contratos SMARTnet. Este contrato del Nivel 2 brinda acceso prioritario a un equipo designado de ingenieros que han recibido capacitación exhaustiva sobre las operaciones comerciales del estadio. Los ingenieros utilizan el Ciclo de vida Cisco como el método para proporcionar servicios desde el momento en que el diseño del estadio se implementa a lo largo del ciclo de vida.

Con el conocimiento sólido de la infraestructura de la red del estadio y el historial de servicios, los ingenieros podrían acelerar la resolución de problemas de red.

9.3.4 Servicios y soporte para el software IOS

Refiera a la **Figura** del curso en línea

Uno de los objetivos comerciales de la compañía de administración del estadio es simplificar la gestión cotidiana de la red del estadio. Para lograr este objetivo, el personal de la CompañíadeRedes recomienda que se instale un software de administración de red.

Servicios de soporte a aplicaciones de software

La implementación de una aplicación de Administración de redes CiscoWorks o de una solución de telefonía IP Cisco requiere productos de software Cisco además del hardware de red. Cisco ofrece Servicios de soporte a aplicaciones de software (SAS) para respaldar el software de aplicación.

Los servicios SAS incluyen acceso las 24 horas a soporte técnico, actualizaciones de software de aplicación y muchísima información técnica en Cisco.com. Los servicios SAS están diseñados específicamente para las aplicaciones de software Cisco y proporcionan servicios además del soporte de software para el sistema operativo.

Los costos de estas opciones de soporte de software y los costos de las licencias de software se incluyen en la propuesta.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Crear la BOM e introducir la información apropiada en la sección Costos de la propuesta de la CompañíaCinematográfica.

9.4 Creación y presentación de la propuesta

9.4.1 Finalización de la propuesta

Refiera a la **Figura** del curso en línea

El gerente de cuentas de la CompañíadeRedes utiliza la información de la implementación que ha finalizado y las secciones de cálculos de costos para actualizar el Resumen ejecutivo. Los componentes de la propuesta se organizan en una carpeta de acuerdo con el pedido mencionado en el Índice.

Al inicio de la propuesta se incluye una portada. La portada contiene información relevante que describe la propuesta, incluso el número y la fecha de la RFP o de la solicitud, la información de contacto del cliente y el nombre y la información de contacto del proveedor.

Al final de la propuesta, se incluyen los términos del contrato y una página de aprobación para que firme el cliente. Los términos y condiciones describen todos los términos legales relevantes y los contratos que se requieren. Estos términos y condiciones respaldan el suministro de bienes y servicios relacionados con mejoras e instalaciones de redes.

Entre las cláusulas importantes de los términos y condiciones se incluyen:

- los detalles de la fecha de vencimiento de la propuesta
- las obligaciones del cliente de obtener permisos u otros consentimientos dentro de su organización
- las obligaciones del proveedor de proporcionar los servicios y los equipos con cuidado y aptitud
- las fechas en las que se deben pagar los materiales meta a entregar finalizados
- el interés a cobrar por pagos insolutos
- la cantidad de tiempo que el cliente tiene para avisar sobre la cancelación de pedidos de equipos o servicios
- los detalles acerca de las garantías (en su caso) proporcionadas por el proveedor
- los detalles sobre el incremento y la resolución de reclamos y problemas

Si el cliente acepta la propuesta, el representante correspondiente del cliente firma la página de Términos y firmas.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Reunir la información sobre la implementación y el cálculo de costos para la CompañíaCinematográfica.

9.4.2 Presentación de la propuesta

Refiera a la **Figura** del curso en línea

Después de recopilar la propuesta, el diseñador de red revisa toda la propuesta junto con la administración de la CompañíadeRedes. Durante esta etapa de la propuesta del diseño, el diseñador debe convencer a la administración interna de la CompañíadeRedes y luego al cliente acerca del concepto.

Generalmente, el diseñador elabora una presentación para ilustrar la propuesta. La presentación de una propuesta incluye diapositivas u otro tipo de medios visuales para representar la propuesta gráficamente. La presentación, junto con el documento de la propuesta, es fundamental para garantizar el éxito de la reunión y aumentar las probabilidades de aprobación por parte del cliente.

La presentación

El contenido y el formato de la presentación son muy importantes en el ambiente empresarial.

Sugerencias para la presentación:

- Cada diapositiva debe incluir un título que resuma la información presentada en la diapositiva.
- Las presentaciones realizadas con computadora no deben contener párrafos enteros de texto. Utilice una lista con viñetas o un formato de esquema y amplíe los puntos durante la presentación.
- Todos los tipos de letra deben ser legibles. Utilice letras grandes porque a veces resulta difícil leer las letras pequeñas.
- Utilice colores que contrasten, ya sea un fondo oscuro con texto claro o un fondo claro con texto oscuro.
- Evite los fondos que dificultan la lectura del texto. Deje un fondo simple.
- ¡No use SÓLO MAYÚSCULAS! Su uso es poco profesional y pueden resultar difíciles de leer.
- Incluya una combinación de palabras, imágenes y gráficos. La variedad ayuda a mantener el interés en la presentación.

Después de la presentación, es posible que el cliente acepte la propuesta en su totalidad, que solicite cambios o que rechace la propuesta por completo.

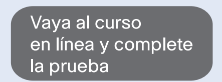
Recuerde que una preparación adecuada antes de la presentación puede significar la diferencia entre la aprobación del cliente y perder el proyecto.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Presente la propuesta del proyecto al instructor y a la clase. Prepárese para responder las preguntas de los instructores y los estudiantes.

Resumen del capítulo



Examen del capítulo

Tome el examen de capítulo para probar su conocimiento.

Sus notas del capítulo

CAPÍTULO 10

Resumen del curso

10.0 Unificación

10.0.1 Resumen

Refiera a la **Figura** del curso en línea

Las redes son fundamentales en casi todas las organizaciones modernas exitosas. Esto es así en casi todas las industrias que se puedan imaginar, incluidas las de asistencia médica, deportes, agencias gubernamentales e ISP. Las aptitudes que ha desarrollado en este curso para las ventas previas y el diseño de la red le proporcionan la base para respaldar cualquier organización de IT o de redes, desde una pequeña empresa de asesoramiento hasta una gran empresa corporativa.

Como profesional de IT, su trabajo será brindar estos servicios de red esenciales de manera eficaz y sin causar problemas a la empresa. Al ejecutar los distintos roles del sistema de redes de manera competente y profesional, se convertirá en un colaborador valioso para cualquier empresa.

La industria de IT mejora y se expande constantemente. Una carrera exitosa en IT requiere de un compromiso con la capacitación constante. La Academia de sistema de redes de Cisco ofrece varios cursos, como el Profesional de sistema de redes certificado de Cisco (CCNP, Cisco Certified Networking Professional), que brindan la capacitación continua que usted necesita.

10.0.2 Cómo encontrar el trabajo apropiado en sistema de redes

Refiera a la **Figura** del curso en línea

Las últimas dos actividades del plan de estudios están diseñadas para respaldar su búsqueda de trabajo en sistemas de redes. La cartera que ha creado durante este curso lo ayudará a evaluar sus aptitudes e intereses. También le servirá como documentación y material de referencia durante su carrera de sistemas de redes.

Hay muchos recursos disponibles para asistirlo en la búsqueda de su carrera: libros, sitios Web, clases y asesores. La mayoría de las instituciones educativas cuentan con recursos disponibles para ayudar a los estudiantes a crear sus currículum vitae, buscar oportunidades de trabajo y practicar entrevistas.

Los empleadores del mundo respetan el plan de estudios y la capacitación para el examen de certificación de la CCNA. Como CCNA calificado, quizá pueda considerar aceptar un puesto fuera de su propio país o un puesto que requiera viajar a otros países. Otra opción es iniciar su propio negocio.

Cuando busque un empleo, debe incluir los siguientes pasos:

- Evalúe sus aptitudes y fortalezas.
- Investigue los tipos de puestos disponibles que requieran sus fortalezas.
- Cree su currículum vitae.
- Envíe su currículum vitae a los posibles empleadores y publíquelo en sitios Web de búsqueda de trabajo en línea.
- Hable con las personas que trabajan en el tipo de puesto que a usted le interesa.

- Hable con las personas que trabajan para compañías que le resultan atractivas.
- Solicite empleos y tenga entrevistas para los puestos disponibles.

Refiera a la **actividad de laboratorio** del curso en línea

Actividad en el laboratorio

Averiguar sobre empleos de sistemas de redes que coincidan con sus aptitudes, fortalezas e intereses.

Elabore un currículum vitae y envíelo con una carta de presentación para un puesto de sistemas de redes que le interese.

Refiera a la **Figura** del curso en línea

Imagine que ha enviado su currículum a una empresa y que le han pedido entrevistarlo.

Tipos de preguntas

Esté preparado para que su entrevistador le realice distintos tipos de preguntas, por ejemplo:

- ***De comportamiento.*** Cómo interactúa con las personas y la cultura en el lugar de trabajo: "¿Está dispuesto a trabajar más horas si es necesario?"
- ***Hipotéticas.*** Cómo manejaría una situación determinada: "¿Qué haría si el edificio se quedara sin energía?"
- ***Guiadas.*** Una serie de preguntas dirigidas a un tipo de situación en particular: "¿Ha trabajado alguna vez en un entorno de laboratorio?"
- ***Abiertas.*** Una pregunta corta que requiere una respuesta extensa: "Cuénteme sobre su experiencia laboral".

Métodos para entrevistar

En las entrevistas, se utilizan muchos métodos diferentes. Entre los métodos comunes se incluyen:

- Una entrevista de evaluación de antecedentes por teléfono
- Una entrevista en una feria de oportunidades profesionales
- Una entrevista con una o más personas en el sitio de la empresa que ofrece el puesto

Una entrevista informativa en la que usted habla con alguien en una empresa en particular. Usted conoce detalles de la empresa y el entrevistador lo conoce a usted. Durante una entrevista informativa no se habla sobre ninguna oportunidad laboral en particular.

Si considera cada entrevista como una experiencia de aprendizaje valiosa, incrementará sus aptitudes para las entrevistas laborales y su conocimiento sobre las prácticas de contratación. Después de la entrevista, reflexione sobre lo que aprendió, qué salió bien y qué desea mejorar para la próxima entrevista.

10.0.3 Preparación para el examen CCNA y capacitación constante

Resumen de pantalla completa.

Sus notas del capítulo

Glosario

3DES

Estándar de encriptación triple de datos.

Procedimiento de protección de datos cuyo primer paso consiste en separarlos en bloques de 64 bits. A continuación, se procesa cada bloque tres veces, cada una, con una clave de 56 bits independiente. El 3DES utiliza una clave de 168 bits en total para garantizar una sólida encriptación. El 3DES es una variación del estándar de encriptación de 56 bits.

802.1q

Estándar de IEEE diseñado para permitir el tráfico entre LAN virtuales. El estándar 802.1q de IEEE utiliza un mecanismo de etiquetado interno que agrega un campo de etiqueta de cuatro bytes en la trama Ethernet original, entre la dirección de origen y los campos de tipo/longitud. Dado que se altera la trama, el dispositivo de enlace troncal vuelve a calcular la secuencia de verificación de trama en la trama modificada.

ABR

Router de borde de área.

Dispositivo de enrutamiento que conecta una o más áreas OSPF a una red backbone. El ABR mantiene tablas de enrutamiento para el backbone y las áreas conectadas de un OSPF.

Acceso protegido Wi-Fi

Ver WPA.

ACK

Acuse de recibo.

Notificación enviada entre dispositivos de red cuando se produce un evento. Por ejemplo, un dispositivo de destino envía un ACK a un dispositivo de origen cuando se recibe un mensaje.

ACL

Lista de control de acceso.

Lista generada por un dispositivo de red, como un router, para administrar el acceso desde el router o hacia él para diversos servicios. Por ejemplo, la ACL puede ser útil para impedir que los paquetes con cierta dirección IP o protocolo salgan de determinada interfaz del router.

ACL basada en tiempo

ACL que permite y rechaza tráfico específico basándose en el momento del día o en el día de la semana. Las ACL basadas en el tiempo son similares en función a la ACL extendida, pero admiten el control de acceso basado en un rango de tiempo. Se crea un rango de tiempo para definir momentos del día y de la semana específicos, a fin de controlar el acceso. El rango de tiempo depende del reloj del sistema del router y funciona mejor con la sincronización del Protocolo de hora de red (NTP).

ACL dinámica
Una ACL que requiere que el usuario utilice Telnet para conectarse al router y llevar a cabo la autenticación. Una ACL extendida bloquea inicialmente el tráfico a través del router. Los usuarios que deseen atravesar el router son bloqueados por la ACL extendida hasta que envían un mensaje de Telnet al router para ser autenticados. En ese momento, se interrumpe la conexión a Telnet, y se agrega una única entrada de ACL dinámica a la ACL extendida existente. Esta entrada permite el tráfico por un período de tiempo determinado; es posible que se produzcan errores por inactividad y superación del tiempo de espera. Las ACL dinámicas a veces se denominan "de bloqueo", porque el usuario debe iniciar sesión a fin de obtener acceso.

ACL estándar
Lista de control de acceso que acepta o rechaza paquetes según la dirección IP de origen. Las ACL estándar están identificadas por el número que se les ha asignado. Los números van del 1 al 99 y del 1300 al 1999.

ACL extendida
Tipo de lista de control de acceso que filtra las direcciones IP de origen, las direcciones IP de destino, las direcciones MAC, el protocolo y los números de puerto. El número de identificación asignado a una ACL extendida puede ser desde 100 hasta 199 y desde 2000 hasta 2699.

ACL reflexiva
Un ACL que permite que se filtren los paquetes IP a partir de la información de la sesión de capa superior. Se usan generalmente para permitir que el tráfico entrante ingrese en una red en respuesta a las sesiones que se originaron en una interfaz dentro del router. Este mecanismo puede ayudar a reducir la exposición a la denegación de servicios y los ataques de suplantación de identidad. Los ACL reflexivos funcionan de manera similar a la palabra clave "establecida" usada en sentencias de ACL extendidas, con la excepción de que los ACL reflexivos pueden inspeccionar también el tráfico UDP y ICMP además del TCP.

Actividad
Broadcast enviado por un dispositivo de red para informar a otro dispositivo de red que el circuito virtual entre ambos sigue estando activo.

Actualización de enrutamiento
Mensaje que se envía desde un router para verificar el acceso a la red y la información de costo asociada. Una actualización de enrutamiento se envía a intervalos regulares y luego de un cambio en la topología de la red.

Actualización flash
Información de enrutamiento enviada de forma asíncrona en respuesta a un cambio en la topología de la red.

Actualización limitada
Función asociada con un protocolo de enrutamiento del estado de enlace, como EIGRP. Una actualización limitada contiene parámetros específicos y se entrega sólo a los routers que requieren esa información.

Actualizaciones de horizonte dividido
Técnica de enrutamiento en la que se evita que la información acerca de una ruta salga de la interfaz del router a través del cual se recibió dicha información. Se utiliza la actualización de horizonte dividido para evitar los routing loops.

Acuerdo de nivel de servicio
Ver SLA.

Acuse de recibo
Ver ACK.

AD
1) distancia publicada

Distancia enviada por broadcast por un vecino ascendente.

2) distancia administrativa

Calificación de la fiabilidad de una fuente de información de enrutamiento. En un router Cisco, la distancia administrativa se expresa por un valor numérico de 0 a 255. Cuanto mayor sea el valor, menor la calificación de fiabilidad.

Administración de dispositivos de seguridad de Cisco
Ver SDM.

Administración de relaciones con el cliente
Ver CRM.

Administrador de comunicaciones unificadas de Cisco
PBX basado en IP en una solución de telefonía IP. El administrador de comunicaciones unificadas de Cisco funciona como agente de llamada para los teléfonos IP y los gateways MGCP. Puede interactuar con dispositivos H.323 o SIP mediante los protocolos de los dispositivos.

El Administrador de comunicaciones unificadas de Cisco también se denomina Administrador de llamadas unificadas de Cisco, o Administrador de llamadas.

Adyacencia
Relación que se establece entre routers vecinos y nodos finales, con el propósito de intercambiar información de enrutamiento. La adyacencia se basa en el uso de un segmento común de medios.

AES
Estándar de encriptación avanzada.

Especificaciones de un cifrado de bloques de 128 bits simétricos que constituye el estándar criptográfico actual en los Estados Unidos, adoptado por el Instituto Nacional de Normas y Tecnología. El algoritmo debe utilizarse con tamaños de clave de 128 bits, 192 bits o 256 bits, de acuerdo con los requisitos de seguridad de la aplicación.

Agente de llamadas
Dispositivo de control que procesa llamadas y administra gateways en la telefonía IP. Un agente de llamadas lleva a cabo funciones similares al conmutador de un sistema telefónico tradicional. Entre los ejemplos de agentes de llamadas, se cuentan el Administrador de comunicaciones unificadas de Cisco y el Administrador de comunicaciones unificadas express de Cisco.

Agente de seguridad de Cisco
Consta de agentes basados en el host, implementados en servidores y equipos de escritorio críticos que dependen del Centro de administración de Cisco para los agentes de seguridad de Cisco. El Centro de administración se ejecuta como aplicación independiente que realiza la configuración de las implementaciones del agente de seguridad de Cisco. Los agentes de seguridad de Cisco proporcionan protección contra amenazas a servidores, equipos de escritorio y equipos portátiles.

Agregación de rutas
Ver sumarización de rutas.

Agrupación de switches de Cisco
Administración de hasta 16 switches simultáneamente mediante una única dirección IP. Para crear redundancia en la agrupación de switches de Cisco, el administrador de red asigna una dirección IP a un segundo switch. Si falla el switch de comando principal, el respaldo o switch de comando secundario se encarga de la administración del grupo sin que se produzcan interrupciones. El usuario aún tiene acceso al grupo mediante la dirección IP virtual.

La tecnología de agrupación de switches de Cisco está presente en los switches Catalyst 3500 XL, 2900 XL, 2955/2950, 2970, 3550, 3560, 3750 y 4500, y en los switches Catalyst 1900/2820 Standard y Enterprise Edition.

Agrupados
Red de servidores utilizados como unidad individual. La redundancia de tecnología que se produce al usar la agrupación mejora el rendimiento gracias al balanceo de carga y a la capacidad de migración entre los dispositivos en caso de fallos.

AH
Encabezado de autenticación.

Protocolo de seguridad que proporciona autenticación de datos y servicios opcionales sin repetición. Este encabezado está incorporado en los datos que deben protegerse.

Algoritmo
Proceso matemático o regla bien definido para la resolución de un problema. En networking, suelen utilizarse los algoritmos para determinar la mejor ruta para el tráfico desde el origen al destino.

Algoritmo de actualización difuso
Ver DUAL.

Algoritmo de Dijkstra
Proceso utilizado en un SPF para identificar todas las rutas a cada destino y el costo total de cada ruta.

Algoritmo de enrutamiento
Fórmula matemática para procedimientos usados para determinar la mejor ruta para enviar el tráfico de origen a destino.

Algoritmo de enrutamiento de estado de enlace
Proceso matemático en el cual cada router envía mediante broadcast o multicast información sobre el costo de alcanzar a cada uno de sus vecinos. Un algoritmo de enrutamiento de estado de enlace crea una visión coherente de la red y no es propenso a los routing loops. Entre los ejemplos de algoritmos de estado de enlace, se incluyen OSPF e IS-IS.

Algoritmo de enrutamiento de vector distancia
Proceso matemático que utiliza la cantidad de saltos de una ruta para descubrir la ruta más corta para llegar a un destino. Los algoritmos de enrutamiento de vector distancia piden que cada router envíe toda su tabla de enrutamiento en cada actualización pero sólo a los routers vecinos. Los algoritmos de enrutamiento de vector distancia son propensos a sufrir routing loops, pero son más simples en cuanto a su cálculo que los algoritmos de enrutamiento de estado de enlace.

Algoritmo shortest path first
Ver algoritmo SPF.

Algoritmo spanning-tree
Proceso matemático que crea un árbol de jerarquía para establecer puentes en una red.

Algoritmo SPF
Algoritmo shortest path first.

Proceso matemático que usa la longitud de una ruta para determinar un spanning tree de ruta más corta. El SPF es un algoritmo de enrutamiento de estado de enlace.

Almacenamiento con conexión a red
Ver NAS.

Almacenar y enviar
Técnica en la que las tramas se procesan completamente antes de ser enviadas a través del puerto adecuado. La conmutación por paquetes de almacenamiento y envío es un proceso que incluye el cálculo de la comprobación de redundancia cíclica y la verificación de la dirección de destino.

Analizador de puerto conmutado
Ver SPAN.

Analizador de red
Dispositivo de monitoreo o aplicación de software que mantiene información estadística con respecto al estado de la red y de cada dispositivo conectado a ésta. Algunos analizadores de red pueden detectar, definir y corregir problemas de red.

Ancho de banda
Capacidad de rendimiento nominal de un medio o un protocolo de red específico. El ancho de banda es la diferencia entre las frecuencias más altas y más bajas disponibles para señales de red.

Ancho de banda de referencia
Parámetro relacionado con la métrica del costo OSPF que se usa para calcular el costo de la interfaz. El cálculo del valor del ancho de banda de cada interfaz utiliza la ecuación 100 000 000/ancho de banda, o 10^8/ancho de banda.

Anycast
Tipo de esquema de enrutamiento y direccionamiento de redes IPv6 en el que los datos se enrutan al destino que se considera el mejor o el más cercano, según la topología de enrutamiento. Una dirección de anycast tiene el mismo formato que una dirección unicast global de IPv6.

AP
Punto de acceso.

Dispositivo de la capa de acceso que se conecta a una red por cable y transmite datos entre dispositivos inalámbricos y conectados por cable. El AP conecta dispositivos de comunicación inalámbrica para formar una red inalámbrica y permitir el roaming.

Aplicación de seguridad
Dispositivo que protege los datos y el hardware contra daños y accesos no deseados.

Aplicación de seguridad adaptable de Cisco
Ver ASA.

Aprendizaje
Uno de los cuatro estados por los que pasa un puerto cuando se enciende un switch en una red STP. El switch utiliza la información reunida para enviar un paquetes.

Árbol SPF
Todas las rutas desde el origen a cada destino y el costo total de cada ruta.

Área
Conjunto lógico de segmentos de red basados en CLNS, DECnet u OSPF, y todos los dispositivos conectados. Por lo general, las áreas se conectan mediante routers y crean un único sistema autónomo.

Área 0
Área inicial de una red OSPF. La red OSPF debe tener al menos un área, que se denomina área 0. A medida que se expande la red, se crean otras áreas adyacentes al área 0.

El área 0 también se denomina área de backbone.

Área de conexión única
Área OSPF que transporta una ruta predeterminada, rutas intra-área y rutas inter-áreas, pero que no transporta rutas externas. No se pueden configurar enlaces virtuales a través de un área de conexión única, y no pueden contener ningún router de borde de sistema autónomo.

Área sin conexión única
Área OSPF que transmite las rutas predeterminadas, estáticas, dentro del área, entre áreas y externas. Un área sin conexión única puede tener vínculos virtuales configurados y puede contener un ASBR.

Armario de cableado
Habitación diseñada especialmente para el cableado de una red de datos o voz. Los armarios de cableado actúan como punto de unión central para el cableado y el equipo de cableado que se usa para interconectar dispositivos.

ARP inverso
Protocolo de resolución de direcciones inverso.

Método para crear rutas dinámicas en una red. El ARP inverso permite que un servidor de acceso detecte la dirección de red de un dispositivo asociado con un circuito virtual.

El ARP inverso también se denomina ARP inverso o RARP.

Arquitectura empresarial de Cisco
Combinación de infraestructura de red central con tecnologías avanzadas de mejora de la productividad, incluidas las comunicaciones IP, la movilidad y la seguridad avanzada. La arquitectura de red empresarial de Cisco divide el diseño jerárquico de tres capas en áreas modulares. Los módulos representan diferente conectividad física o lógica. También designan las diferentes funciones que se producen en la red. La modularidad de la arquitectura de red empresarial de Cisco permite flexibilidad en el diseño de la red y facilita la implementación y la resolución de problemas.

Arquitecturas de redes empresariales
Red que integra todos los sistemas dentro de una empresa u organización. Una red empresarial se diferencia de una WAN en el sentido de que pertenece y se mantiene en forma privada.

Arquitecturas empresariales de Cisco
Combinación de infraestructura de red central con tecnologías avanzadas de mejora de la productividad, incluidas las comunicaciones IP, la movilidad y la seguridad avanzada. La arquitectura de red empresarial de Cisco divide el diseño jerárquico de tres capas en áreas modulares. Los módulos representan diferente conectividad física o lógica. También designan las diferentes funciones que se producen en la red. La modularidad de la arquitectura de red empresarial de Cisco permite flexibilidad en el diseño de la red y facilita la implementación y la resolución de problemas.

AS
Sistema autónomo.

Conjunto de redes bajo una administración común que comparten una estrategia de enrutamiento común. Los sistemas autónomos se subdividen por áreas. IANA le debe asignar un número exclusivo de 16 bits al sistema autónomo.

ASA
Aplicación de seguridad adaptable de Cisco.

Dispositivo de hardware que integra un firewall, seguridad de comunicaciones unificadas, VPN de SSL e IPsec, IPS y servicios de seguridad de contenidos. Un ejemplo de una aplicación ASA es la serie ASA 5500 de Cisco.

ASBR
Router de borde del sistema autónomo.

Router de borde de área ubicado entre un sistema autónomo de OSPF y una red no perteneciente a OSPF. El ASBR ejecuta el protocolo de enrutamiento OSPF y otro protocolo de enrutamiento, como RIP. Los ASBR deben residir en un área OSPF sin conexión única.

Ascendente
Técnica de resolución de problemas que examina, en primer lugar, los niveles inferiores de un modelo jerárquico.

ASIC
Circuito integrado de aplicación específica.

Circuito que proporciona instrucciones precisas para la funcionalidad de un dispositivo durante la conmutación de Capa 3.

Asignación dinámica de canales
Asignación dinámica de canales.

Frecuencia de radio abierta que se selecciona cuando un punto de acceso identifica un canal no utilizado en una WLAN.

Asimétrica
Una función de la red que demora más tiempo que la función inversa. Un ejemplo de una función asimétrica es la compresión y descompresión de datos.

Ataque de repetición
Proceso malicioso que permite que un pirata informático obtenga acceso a un router usando información que éste graba y repite como prueba de identidad.

ATM
Modo de transferencia asíncrona.

Estándar internacional para relay de celdas de tipos de servicios, tales como voz, video o datos. En este modo, los servicios se transmiten en celdas de longitud fija de 53 bytes. Las celdas de longitud fija reducen las demoras en el tránsito, dado que el procesamiento de celdas se lleva a cabo en el hardware. El ATM está diseñado para medios de transmisión de alta velocidad, por ejemplo, E3, SONET y T3.

Autenticación
Medida de seguridad diseñada para controlar el acceso a los recursos de la red que verifica la identidad de una persona o proceso.

Autenticación de contraseña simple
Método que ofrece seguridad básica a un router usando una clave para obtener acceso.

AutoQoS
Función que automatiza la implementación coherente de las funciones de calidad del servicio en los switches y routers de Cisco para garantizar el rendimiento óptimo de las aplicaciones. AutoQoS configura el dispositivo con funciones de calidad de servicio y variables basadas en las recomendaciones de mejores prácticas de Cisco. Los parámetros generados por la función AutoQoS de Cisco pueden ser configurados por el usuario.

Autoridad de números asignada por Internet
Ver IANA.

Backbone colapsado
Sistema de medios físicos en el que todos los segmentos de la red están interconectados por un dispositivo de internetworking. Un ejemplo de un backbone colapsado es un segmento de red virtual que existe en un dispositivo como un hub, un router o un switch.

Backbone de la red
Arquitectura del núcleo de una red empresarial. El backbone de la red conecta todos los segmentos de la LAN de un sistema y proporciona conmutación rápida entre subredes.

Back-end
Aplicación que lleva a cabo funciones finales u ocultas en un proceso.

BackboneFast
Función de los switches de una red puente que proporciona convergencia rápida luego de un cambio en la topología de Spanning Tree. BackboneFast se utiliza en las capas de distribución y core a fin de restaurar la conectividad de backbone. BackboneFast es una tecnología patentada de Cisco.

Balanceo de carga
La capacidad de un router para distribuir tráfico a través de todas las interfaces de red que están a la misma distancia de la dirección de destino. El balanceo de carga aumenta el uso de los segmentos de red, lo que mejora el ancho de banda. Un algoritmo de balance de carga puede utilizar información de la velocidad de línea y de la fiabilidad.

Balanceo de carga con distinto costo
Distribución de paquetes entre más de una ruta usando una variación específica de la métrica. La distribución del tráfico impide que una ruta se sobrecargue.

Balanceo de carga de mismo costo
Técnica de distribución de paquetes admitida por EIGRP para evitar la sobrecarga de una ruta de red.

Banner motd
Banner motd.

Comando utilizado para configurar el mensaje del día, o motd (message of the day). El mensaje se muestra al iniciar sesión. El comando banner motd es útil para transmitir mensajes que afectan a todos los usuarios de la red, como un aviso sobre una interrupción inminente del sistema.

Base de datos de topología
Ubicación en una topología que almacena información del árbol SPF.

Base de información de administración
Ver MIB.

Baudio
Unidad de velocidad de señalización que es igual a la cantidad de elementos discretos de la señal transmitidos por segundo. Baudio es sinónimo de bits por segundo, si cada elemento de la señal representa exactamente 1 bit.

Bc
Ráfaga suscrita.

Cantidad máxima de datos en bits que una internetwork Frame Relay se compromete a aceptar y transmitir a la CIR. Bc es una métrica negociada de tarifas.

BDR
Router designado de respaldo.

Router identificado para llevar a cabo las funciones del router designado si éste falla.

Be
Ráfaga excesiva.

Cantidad de bits que una internetwork Frame Relay intenta transmitir luego de que se ha enviado la Bc. Los datos Be, en general, tienen una probabilidad menor de ser entregados que los datos Bc dado que los datos Be se pueden marcar como DE por la red. Be es una métrica negociada de tarifas.

BECN
Notificación explícita de congestión hacia atrás.

Señal de una trama que viaja en dirección opuesta a las tramas que encuentran una ruta congestionada en una red Frame Relay. El DTE que recibe la trama con la señal de BECN puede solicitar que se lleve a cabo una acción de control de flujo por parte de los protocolos de nivel superior.

BGP
Protocolo de border gateway.

Estándar de enrutamiento que se utiliza para conectar un SP a Internet y desde ésta.

El BGP también se conoce como protocolo de Gateway exterior.

BID
ID de puente.

Identificación del puente raíz que constituye el punto focal en una red STP.

Bloque de switch
Configuración en la cual un router, o switch multicapa se distribuye en pares, con los switches de capa de acceso divididos equitativamente entre ellos. Cada bloque de switch actúa independientemente, lo cual impide que la red se desconecte si falla un dispositivo.

El bloque de switch también se denomina bloque de switch departamental o de creación.

Bloqueo
1) En un sistema de conmutación, una condición en la que no hay ninguna ruta disponible para completar un circuito. 2) Condición en la que una actividad no puede comenzar hasta que se lleve a cabo otra.

Bloques de switch
Configuración en la cual un router, o switch multicapa se distribuye en pares, con los switches de capa de acceso divididos equitativamente entre ellos. Cada bloque de switch actúa independientemente, lo cual impide que la red se desconecte si falla un dispositivo.

El bloque de switch también se denomina bloque de switch departamental o de creación.

BOM
Lista de materiales.

Lista detallada de hardware, software y otros elementos necesarios para desarrollar una red. La BOM se utiliza para obtener cotizaciones de precios y solicitar equipos.

BPDU
Unidad de datos del protocolo de puentes.

Paquete de saludo del protocolo del spanning-tree que se envía a intervalos configurables para intercambiar información entre los puentes de la red.

Broadcast
Conjunto de dispositivos que recibe tramas de broadcast que tienen su origen en cualquiera de los dispositivos dentro del conjunto. Los dominios de broadcast generalmente están limitados por routers, dado que éstos no envían tramas de broadcast.

Bucle
En una red, ruta en la que un paquete nunca llega a destino. El bucle transmite los datos repetidamente a través de una serie constante de nodos de red.

Bucle de conmutación
Ocasiona que se envíen tramas duplicadas por una red. Un bucle de conmutación ocurre cuando hay más de una ruta entre dos switches.

Bucle local
Línea física desde las instalaciones o punto de demarcación de un suscriptor telefónico hasta el extremo de la oficina central de la portadora o compañía telefónica.

Un bucle local también se conoce como línea de suscriptor.

Búfer
Área de almacenamiento que se usa para administrar los datos en tránsito. En internetworking, los búferes se usan para compensar las diferencias de las velocidades de procesamiento entre los dispositivos de red. Las ráfagas de datos se pueden guardar en búfer hasta que los datos puedan ser administrados por dispositivos de procesamiento más lento.

Un búfer también se conoce como búfer de paquetes.

Búsqueda recurrente
Dos pasos necesarios para determinar la interfaz de salida. En primer lugar, un router hace coincidir la dirección IP de destino de un paquete con la ruta estática. Luego, hace coincidir la dirección IP del siguiente salto de la ruta estática con las entradas de su tabla de enrutamiento para determinar qué interfaz debe utilizar.

Cable de conexión cruzada
Estilo de conexión de switches y hubs para que puedan enviar y recibir datos.

Cable de fibra óptica
Medio físico que puede conducir una transmisión de luz modulada. Si se compara con otros medios de transmisión, el cable de fibra óptica es más caro y es capaz de brindar velocidades de datos más altas; sin embargo, no es susceptible a la interferencia electromagnética.

El cable de fibra óptica también se conoce como fibra óptica.

Cableado backbone
Medios físicos que conectan armarios para el cableado entre sí, armarios para el cableado y el POP, y edificios que forman parte de la misma LAN.

Cableado estructurado
Uso de un estándar reconocido internacionalmente para implementar un diseño de cableado de red física.

Caché
Acto de almacenar datos o la ubicación de los datos almacenados.

Cadena de cifrado
Forma encriptada de texto sin formato.

Calidad de servicio
Ver QoS.

CAM
Memoria de contenido direccionable.

Tabla de direcciones MAC mantenida por un switch. Se vuelve a crear una CAM cada vez que se activa un switch.

Campo de tipo
Campo extra en una trama HDLC Cisco que permite que múltiples protocolos compartan el mismo enlace al indentificar el tipo de protocolo enviado por la trama.

Canal
Ruta de comunicación que puede multiplexarse en un solo cable.

Capa de acceso
Nivel del modelo de internetworking jerárquico de Cisco que comprende los hosts que funcionan como punto de ingreso a la red. Los dispositivos de capa de acceso incluyen switches, hubs, estaciones de trabajo, servidores, teléfonos IP, cámaras Web y puntos de acceso.

Capa de aplicación
La capa 7 del modelo de referencia OSI. La capa de aplicación suministra servicios a los procesos de aplicación (por ejemplo, correo electrónico, transferencia de archivos y emulación de terminal) que están fuera del modelo de referencia de OSI. Identifica y establece la disponibilidad de los socios de comunicaciones deseados (y los recursos necesarios para conectarse con ellos), sincroniza las aplicaciones colaboradoras y establece acuerdos con respecto a los procedimientos para la recuperación de errores y el control de la integridad de los datos.

Capa de distribución
Capa que se encuentra entre la capa de acceso y la capa núcleo en un diseño jerárquico. La capa de distribución interconecta los hosts de la capa de acceso y los switches, y proporciona administración del tráfico y de la seguridad para la capa núcleo.

Capa núcleo
Capa perteneciente a un diseño jerárquico de tres capas, junto con la de acceso y la de distribución. La capa núcleo representa una capa de backbone de alta velocidad entre redes finales dispersas geográficamente.

Caracterización de la aplicación
Información sobre el uso del ancho de banda de la red y los plazos de respuesta de una aplicación. Algunas de las consideraciones para la caracterización de una aplicación incluyen el funcionamiento de la aplicación, su interacción en una red y los requisitos técnicos.

Carga
Cantidad de tráfico en una red.

Caso comercial
Documento de diseño estructurado generado para justificar la inversión financiera necesaria para implementar un cambio de tecnología.

CBWFQ
Cola equitativa ponderada basada en clases.

Técnica de priorización de paquetes de red basada en la práctica estándar de colas equitativas ponderadas. La CBWFQ tiene funciones adicionales de calidad de servicio que asignan paquetes a clases de tráfico definidas por el usuario. Cada clase recibe un nivel de prioridad según los criterios de coincidencia que incluyen los protocolos, las ACL y las interfaces de entrada.

CCITT
Comité Consultivo Internacional Telegráfico y Telefónico

Organización internacional responsable del desarrollo de los estándares de comunicaciones. El CCITT ahora se denomina ITU-T.

CDP
Protocolo de descubrimiento de Cisco.

Protocolo de equipos fabricados por Cisco, incluidos routers, servidores de acceso, puentes y switches, que permiten que el dispositivo se comunique con otros dispositivos de LAN o del extremo remoto de una WAN. El CDP se ejecuta en LAN, Frame Relay y medios ATM.

Centro de datos
Ubicación de administración central que controla todos los recursos de red.

Un centro de datos también se denomina NOC.

Centro de operaciones de red
Ver NOC.

CHAP
Protocolo de autenticación de intercambio de señales.

Característica de seguridad que se admite en las líneas que usan encapsulación PPP a fin de evitar el acceso no autorizado mediante la identificación del usuario remoto. CHAP es un protocolo de enlace de tres vías con encriptación que permite al router o servidor de acceso determinar si un usuario tiene el acceso permitido.

Ciclo
Proceso que se repite.

CIDR
Enrutamiento entre dominios sin clase.

Técnica basada en la agregación de rutas y compatible con el protocolo de border gateway v4, que permite a los routers agrupar las rutas a fin de reducir la cantidad de información transmitida por los routers núcleo. Al utilizar CIDR, varias redes IP aparecen como una única entidad más extensa ante las redes que se encuentran fuera del grupo.

Cifrado de bloques
Método de encriptación de un grupo de bits como una una sola unidad.

CIR
Velocidad de información suscrita.

Velocidad a la que una red Frame Relay transfiere información, medida en bits por segundo y promediada de acuerdo con un incremento mínimo de tiempo. CIR es una métrica negociada de tarifas.

CIR cero
Exceso de ancho de banda que se descuenta cuando está disponible en un proveedor de servicios de Frame Relay. Con CIR cero, el usuario paga una tarifa reducida por la capacidad de transferir datos a través de un PVC hasta la velocidad del enlace de acceso. Si hay congestión, se descartan todas las tramas con la etiqueta DE. No hay garantía de servicio con un CIR establecido en cero.

Circuito
Ruta de comunicación entre dos o más puntos.

Circuito integrado de aplicación específica
Ver ASIC.

Circuito virtual
Circuito virtual.

Relación lógica que se crea para garantizar la comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por un par identificador de ruta virtual/identificador de canal virtual, y puede ser tanto un circuito virtual permanente como un circuito virtual conmutado. Los circuitos virtuales se usan en Frame Relay y X.25. En ATM, un circuito virtual se denomina canal virtual.

Circuito virtual conmutado
Ver SVC.

Circuito virtual permanente
Ver PVC.

CiscoView
Aplicación para administración basada en GUI que brinda estado dinámico, estadísticas y amplia información acerca de la configuración para los dispositivos de internetworking de Cisco. Además de suministrar una vista física del chasis del dispositivo Cisco, CiscoView también brinda funciones de monitoreo de dispositivos y capacidades básicas de resolución de problemas, y se puede integrar con varias de las plataformas de administración de red basadas en SNMP.

CiscoWorks
Serie de aplicaciones de administración de internetworking basadas en SNMP que se utilizan para monitorear el estado del router y del servidor de acceso, administrar los archivos de configuración y resolver los problemas de red. Las aplicaciones CiscoWorks se integran en varias plataformas, entre ellas, SunNet Manager, HP OpenView e IBM NetView.

Clave
Código de autenticación que se transmite entre routers como texto sin formato.

Clave simétrica
Clave criptográfica que se usa en un algoritmo criptográfico simétrico.

CLI
Interfaz de línea de comandos.

Capacidad de interactuar con el sistema operativo que requiere que el usuario introduzca comandos y argumentos opcionales en una línea de comandos.

Cliente
Dispositivo que solicita servicios o información.

Cliente a cliente
Desde una estación terminal a otra estación terminal en una red.

Cliente a extremo empresarial
Desde una estación terminal al perímetro de la empresa antes de entrar en Internet.

Cliente a granja de servidores
Desde un usuario final a una ubicación con varios servidores.

Cliente a servidor distribuido
Desde una estación terminal al servidor.

Clúster
Red de servidores utilizados como unidad individual. La redundancia de tecnología que se produce al usar la agrupación mejora el rendimiento gracias al balanceo de carga y a la capacidad de migración entre los dispositivos en caso de fallos.

CO
Oficina central.

Entorno ubicado estratégicamente que aloja a los dispositivos vitales en una topología de la red.

Codificación
1. Proceso utilizado para representar bits como voltajes en cables o pulsos de luz en fibra óptica.

2. Técnica eléctrica que se usa para transmitir señales binarias.

Codificador
Dispositivo que modifica la información al formato de transmisión requerido.

Cola de latencia baja
Ver LLQ.

Cola de transmisión
Ver TxQ.

Cola equitativa ponderada basada en clases
Ver CBWFQ.

cola personalizada
Ver CQ.

Cola según prioridad
Ver PQ.

Colisión
Consecuencia cuando dos o más dispositivos transmiten tramas simultáneamente, que chocan y resultan dañadas cuando se encuentran en el medio físico.

Coloreado en rojo
Marcas en un anteproyecto que muestran los cambios de diseño.

Comité Consultivo Internacional Telegráfico
Ver CCITT.

Compañía
Entorno corporativo de gran extensión, con muchos usuarios y ubicaciones, o con muchos sistemas.

Comprobación de redundancia cíclica
Ver CRC.

Con clase
Tipo de división en subredes que utiliza la extensión de la máscara de subred. Un ejemplo de división en subredes con clase es el protocolo IPv4.

Concentrador de VPN
Concentrador de red privada virtual.

Gateway de una red que filtra todo el tráfico de la VPN.

Conexión cruzada horizontal
Ver HCC.

Conexión cruzada principal
Ver MCC.

Conexión de ruta virtual
Ver VPC.

Conexión remota
Ver rlogin.

Configuración básica
Información de configuración mínima que se introduce cuando se instala un router, switch u otro dispositivo configurable en una red. Por ejemplo, la configuración básica del switch ATM LightStream 2020 incluye las direcciones IP, la fecha y los parámetros para al menos una línea troncal. La configuración básica permite que el switch reciba una configuración completa del sistema de administración de la red.

Configuración fija
Las reglas establecidas no pueden alterarse. Un ejemplo de configuración fija es un switch de Capa 2 que tiene el número y el tipo de los puertos, tales como FastEthernet y Gigabit Ethernet, preconfigurados de fábrica.

Conformación del tráfico
Uso de colas para limitar las ráfagas de alto tráfico que pueden congestionar una red. En la conformación de tráfico, los datos se colocan en un búfer y luego se envían a la red en cantidades reguladas, para garantizar que el tráfico se encuadre dentro del tráfico prometido para esa conexión en particular. La conformación de tráfico se usa en redes como ATM y Frame Relay.

Congestión
Tráfico que excede la capacidad de la red.

Conjunto de reglas del firewall
Conjunto de comandos de configuración incluido en la lista de acceso de una aplicación de seguridad de Cisco o en un router Cisco que lleva a cabo funciones de firewall. Las direcciones IP de origen y destino, los protocolos o las funciones de un protocolo pueden verse afectadas por las reglas del firewall.

Conmutación de Capa 3
Proceso de un router que utiliza técnicas de conmutación por método de corte para incrementar la velocidad del envío y la inspección de paquetes.

Conmutación de circuitos
Sistema en el que existe un circuito físico dedicado entre el emisor y el receptor durante la conexión. La conmutación de circuitos se utiliza con frecuencia en las redes de compañías telefónicas.

Conmutación de paquetes
Método de networking en el que los nodos comparten el ancho de banda enviándose paquetes entre sí. La conmutación de paquetes es una forma de dirigir información codificada en una red desde su origen hasta su destino.

Conmutación de paquetes por almacenamiento y envío
Técnica en la que las tramas se procesan completamente antes de ser enviadas a través del puerto adecuado. La conmutación por paquetes de almacenamiento y envío es un proceso que incluye el cálculo de la comprobación de redundancia cíclica y la verificación de la dirección de destino.

Conmutación de paquetes por método de corte
Proceso en que los datos se dirigen a través de un switch de modo que el extremo inicial de un paquete salga del switch en el puerto de salida, antes de que el paquete termine de ingresar al puerto de entrada. La conmutación de paquetes por método de corte permite a un dispositivo leer, procesar y enviar paquetes en cuanto se detecta la dirección de destino y se determina el puerto de salida.

La conmutación de paquetes por método de corte también se denomina conmutación instantánea de paquetes. Ver la diferencia con la conmutación de paquetes por almacenamiento y envío.

Conmutación de proceso
Operación que se lleva a cabo cuando un router evalúa la ruta y el balanceo de carga por paquete de enlaces paralelos antes de enviar un paquete. En la conmutación de procesos, un router lleva a cabo una búsqueda de cada paquete en la tabla, selecciona una interfaz y busca la información del enlace de datos. Dado que la decisión de enrutamiento de cada paquete es independiente, no todos los paquetes con el mismo destino son forzados a utilizar la misma interfaz.

Conmutación multicapa
Dispositivo que filtra y envía paquetes basándose en direcciones MAC y direcciones de red. Un switch de Capa 2/Capa 3 es un switch multicapa.

Conmutación por método de corte
Proceso en que los datos se dirigen a través de un switch de modo que el extremo inicial de un paquete salga del switch en el puerto de salida, antes de que el paquete termine de ingresar al puerto de entrada. La conmutación de paquetes por método de corte permite a un dispositivo leer, procesar y enviar paquetes en cuanto se detecta la dirección de destino y se determina el puerto de salida.

La conmutación de paquetes por método de corte también se denomina conmutación instantánea de paquetes. Ver la diferencia con la conmutación de paquetes por almacenamiento y envío.

Conmutación por silicio
Conmutación dedicada por paquetes de alta velocidad basada en un motor de conmutación de silicio y no en un procesador de switch de silicio.

Conmutación rápida
Función desarrollada por Cisco que utiliza una memoria caché de conmutación de alta velocidad para acelerar la conmutación de paquetes en el enrutamiento de IP. Las direcciones IP de destino se almacenan en la memoria caché, a fin de acelerar el proceso de envío de paquetes.

Contenido de seguridad encapsulado
Ver ESP.

Conteo de saltos
Métrica de enrutamiento que rastrea la cantidad de tramos que debe atravesar un paquete de datos entre el origen y el destino. El RIP usa el conteo de saltos como su única métrica.

Contiguo
Ubicación de un dispositivo vecino. Contiguo significa adyacente o próximo.

Continuidad de la empresa
Posibilidad de continuar las operaciones comerciales en caso de que ocurra un desastre natural o provocado por el hombre.

Control de acceso a la red
Límite de acceso a los componentes físicos de la red.

Control de admisión a la red
Ver NAC.

Control de energía de transmisión
Modifica la transmisión RF en una LAN inalámbrica mediante el aumento o la disminución de la tasa de energía en un dispositivo, para mejorar la calidad del enlace y las señales recibidas.

Control de enlace de datos de alto nivel
Ver HDLC.

Control de enlace de datos de alto nivel (HDLC, High-level Data Link Control)
Control de enlace de datos de alto nivel.

Protocolo de capa de enlace de datos síncrono, orientado a bits, desarrollado por ISO. HDLC especifica un método para encapsular datos en enlaces seriales síncronos usando caracteres de trama y checksums.

Control del flujo
Capacidad de mantener la velocidad de actividad en una red.

Controlador de LAN inalámbrica
Tipo de módulo que proporciona un sistema inalámbrico seguro de clase empresarial. Un controlador de LAN inalámbrica permite que una organización pequeña pueda implementar y administrar una WLAN segura de forma fácil y económica.

Convergencia
Condición donde la velocidad y la capacidad de un grupo de dispositivos de networking que ejecutan un protocolo de enrutamiento específico acuerdan sobre la topología de una internetwork después de que se produce un cambio en dicha topología.

Converger
Condición donde la velocidad y la capacidad de un grupo de dispositivos de networking que ejecutan un protocolo de enrutamiento específico acuerdan sobre la topología de una internetwork después de que se produce un cambio en dicha topología.

Conversor de medios
Proceso de la capa de enlace de datos en un router, que transforma una trama en Ethernet si se encuentra en una LAN, y en interfaz de WAN si sale de la LAN y entra a Internet.

Correo electrónico
Servicio de correo electrónico.

1) Aplicación de red muy utilizada en la que los mensajes de correo se transmiten electrónicamente entre los usuarios finales a través de una red, mediante diversos protocolos de red.
2) Intercambio de mensajes almacenados en computadoras por medio de comunicación de red.

Costo

Valor, generalmente basado en el conteo de saltos, ancho de banda de los medios u otras medidas, que se asigna a través de un administrador de la red y se utiliza para comparar varias rutas a través de un entorno de internetwork. Los protocolos de enrutamiento usan los valores de costo para determinar la ruta más favorable hacia un destino en particular: Cuanto menor sea el costo, mejor la ruta.

El costo también se denomina costo de ruta.

Coubicados
Presentes también en un lugar. Un servidor secundario puede estar coubicado en el mismo SP para respaldo.

CPE
Equipo local del cliente.

Equipo terminal, por ejemplo terminales, teléfonos y módems, suministrado por la compañía telefónica, instalado en las instalaciones del cliente y conectado a la red de la compañía telefónica.

CQ
Cola personalizada.

Método que garantiza el ancho de banda para el tráfico asignando un espacio a cada protocolo.

CRC
Comprobación de redundancia cíclica.

Técnica de comprobación de errores de almacenamiento y reenvío que cuenta la cantidad de paquetes que genera la checksum del dispositivo remoto y la compara con la checksum calculada a partir de los datos recibidos. Un error de CRC puede indicar ruido, picos de ganancia o problemas de transmisión en el vínculo o interfaz de datos.

Creación de superredes
Proceso de resumen de direcciones de clase contiguas establecido por la comunidad de Internet. Un ejemplo de creación de superredes es cuando un grupo direcciones de clase C del 200.100.16.0 al 200.100.31.0 se resume en la dirección 200.100.16.0 con una máscara 255.255.224.0.

También se denomina enrutamiento entre dominios sin clase.

Criptografía
Proceso consistente en transformar texto sin formato en texto cifrado.

Criptografía simétrica
Tipo de codificación de datos que involucra algoritmos que usan la misma clave para dos pasos separados del proceso. Entre los ejemplos de criptografía simétrica se incluyen la encriptación y desencriptación, y la creación y verificación de firmas.

CRM
Administración de relaciones con el cliente.

Software utilizado para ayudar a las organizaciones a captar y retener clientes a fin de lograr crecimiento y expansión.

CSU
Unidad de servicio de canal.

Dispositivo de interfaz digital que conecta el equipo del usuario final con el bucle telefónico digital local. A menudo se denomina, en forma conjunta con DSU, CSU/DSU.

CSU/DSU
Unidad de servicio de canal/unidad de servicio de datos.

Dispositivos de red que conectan una organización a un circuito digital.

Cuarto de telecomunicaciones
Instalación que contiene el equipo de telecomunicaciones y de red, terminaciones de cables verticales y horizontales y cables de la conexión cruzada.

También se lo denomina armario de cableado, instalación de distribución o instalación vertical.

Cuenta a infinito
Situación en que los routers incrementan continuamente el conteo de saltos a redes particulares cuando los algoritmos de enrutamiento tienen una convergencia lenta. Generalmente, se impone un límite arbitrario en el conteo de saltos para evitar la cuenta a infinito.

Código de autenticación de mensajes basado en hash
Ver HMAC.

Código de autenticación de mensajes de hash: algoritmo de hash seguro
Ver HMAC-SHA-1.

Código de autenticación de mensajes de hash: Message Digest
Ver HMAC-MD5.

Datagrama
Unidad de información de una red que contiene las direcciones de origen y destino.

También se lo conoce como mensaje, paquete, segmento o trama.

Datos segmentados
Porciones pequeñas y uniformes de datos que se conmutan rápida y eficientemente entre nodos.

DCA
Asignación dinámica de canales.

Frecuencia de radio abierta que se selecciona cuando un punto de acceso identifica un canal no utilizado en una WLAN.

DCE
Equipo de comunicación de datos.

Conexión física a una red de comunicaciones en un entorno de expansión EIA. El DCE envía tráfico y proporciona una señal de temporización que se usa para sincronizar la transmisión de datos entre los dispositivos DCE y DTE. Entre los ejemplos de dispositivos DCE se incluyen un módem y una tarjeta de interfaz.

DCE también se denomina equipo de terminación de circuitos de datos cuando se lo utiliza en un entorno de expansión ITU-T.

DE
Elegible para descarte.

Designación de un paquete en networking Frame Relay. Un paquete con el bit DE configurado es el primero en ser descartado cuando un router detecta congestión en la red. El bit DE se configura en el tráfico sobresuscrito (es decir, el tráfico recibido después de alcanzar la CIR).

Demarc
Punto indicado entre los equipos de la portadora y el CPE.

Demodulación
Proceso utilizado para devolver una señal modulada a su forma original. Los módems ejecutan demodulación al tomar una señal analógica y convertirla a su forma digital.

Demodular
Proceso utilizado para devolver una señal modulada a su forma original. Los módems ejecutan demodulación al tomar una señal analógica y convertirla a su forma digital.

Denegación de servicio
Ver DoS.

Denegación implícita
Última declaración de un ACL, agregada a fin de bloquear la entrada accidental de tráfico no deseado.

Denegar
Rechazar datos en una red.

Densidad de puertos
Cantidad de puertos por RU en un switch.

Dentro de banda
Técnica de administración de la conexión entre una computadora y un dispositivo de red. La administración dentro de banda se utiliza para monitorear y hacer cambios de configuración en un dispositivo de red a través de una conexión de red.

DES
Estándar de cifrado de datos.

Sistema de encriptación de clave simétrica que utiliza una clave de 56 bits para garantizar una encriptación de alto rendimiento. El DES es un algoritmo criptográfico desarrollado por la Oficina Nacional de Normas de los Estados Unidos. En la actualidad, el gobierno de los Estados Unidos ya no considera que DES sea un algoritmo de encriptación sólida.

Descarte
Estado de un puerto en una red RSTP cuando el servidor no envía una respuesta. Un LED de color ámbar sin parpadeo significa que se está llevando a cabo el descarte.

Descendente
Método de prueba de red diseñado para admitir determinadas aplicaciones y requerimientos de servicio de redes. Cuando se completa un diseño, se realiza una prueba piloto usando el enfoque descendente para garantizar que el nuevo diseño funcione como se espera, antes de su implementación.

Descubrimiento de redes
Resultado del hecho de que los protocolos de enrutamiento dinámico permitan a un router compartir información sobre su alcance y su estado, y también agregar redes remotas a la tabla de enrutamiento.

Desmultiplexación
Acto de separar una señal física común en diversos flujos de salida.

DH
Diffie-Hellman.

Método de intercambio de claves públicas que proporciona una forma para que dos pares establezcan una clave secreta compartida en una ruta de comunicación no segura.

DHCP
Protocolo de configuración dinámica de host.

Estándar utilizado por una utilidad de software que solicita y asigna la dirección IP, el gateway predeterminado y la dirección de servidor DNS a un host de la red. El DHCP asigna una dirección IP de forma dinámica, de modo que la dirección pueda volver a utilizarse cuando los hosts ya no la necesiten.

Diagrama de bloques modulares
Ilustración de las funciones principales de una red en forma modular. El diagrama de bloques modulares ayuda a un diseñador a determinar la arquitectura subyacente que sirve como base de la red.

Diagrama de infraestructura de la red
Ilustración de la topología de una red que muestra la ubicación, la función y el estado de los dispositivos. Un diagrama de infraestructura de la red puede representar una red física o lógica.

Un diagrama de infraestructura de red también se denomina diagrama de topología.

Diámetro de red
Cantidad máxima de saltos entre dos estaciones determinadas de la red. El diámetro de red es la cantidad máxima de enlaces que deben atravesarse para enviar un mensaje a cualquier host mediante la ruta más corta.

Diffie-Hellman
Ver DH.

Dirección
Estructura de datos utilizada para identificar una entidad exclusiva, como ser, un proceso o dispositivo de red particular. La dirección IP es una cadena de caracteres asignada por un administrador. La dirección MAC está grabada en el dispositivo y no se puede modificar.

Dirección de broadcast
Dirección que se reserva para enviar un mensaje a todas las estaciones. Por lo general, una dirección de broadcast es una dirección MAC destino compuesta por todos unos.

Dirección de control de acceso al medio
Ver dirección MAC.

Dirección de helper (ayudante)
Configuración de router que se utiliza para enviar tráfico de red desde una computadora cliente ubicada en una subred a un servidor ubicado en otra subred. La dirección de helper se configura en una interfaz.

Dirección de protocolo de Internet
Ver dirección IP.

Dirección de red privada
Parte de una dirección IP que se reserva para uso interno. Una dirección de red privada no se enruta a través de la Internet pública. En IPv4, el rango de direcciones de red privadas es de 10.0.0.0 a 10.255.255.255, 172.16.0.0 a 172.31.255.255 y 192.168.0.0 a 192.168.255.255.

Dirección de red pública
Dirección IP única y enrutable a través de Internet pública.

Dirección de subred
Parte de una dirección IP que se especifica como la subred a través de la máscara de subred.

Dirección extendida universal de 64 identificadores
Ver EUI-64.

Dirección global externa
Dirección IP pública de un host externo, como se lo denomina en Internet.

Dirección global interna
Dirección IP enrutable para el público de un host interno como aparece en la red externa. La dirección global interna es una dirección IP traducida por la NAT.

Dirección IP
Dirección de protocolo de Internet.

Dirección de 32 bits en IPv4 que se asigna a los hosts que utilizan TCP/IP. La dirección IP pertenece a una de cinco clases: A, B, C, D o E.

Está escrita con cuatro octetos en formato separado por puntos <a.b.c.d>. Cada dirección está compuesta por un número de red, un número de subred opcional y un número de host. Los números de red y subred se utilizan en forma conjunta para el enrutamiento. El número de host se utiliza para direccionar un host individual dentro de la red o subred. La máscara de subred se usa para extraer información de red y subred de la dirección IP.

Dirección local externa
Dirección IP de un host externo según aparece a la red interna.

Dirección local interna
Dirección IP privada configurada en un host dentro de una red interna. Una dirección local interna debe traducirse antes de poder transmitirse fuera de la estructura de direccionamiento a Internet.

Dirección MAC
Dirección de control de acceso al medio.

Dirección de capa de enlace de datos estandarizada que se requiere para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para localizar puertos específicos en la red y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC tienen 6 bytes de largo y se controlan a través de la IEEE.

También denominada dirección de hardware, dirección de capa MAC o dirección física.

Dirección unicast global
Dirección IPv6 única que puede enrutarse a todo el mundo sin modificaciones. Una dirección unicast global comparte el mismo formato de dirección que una dirección anycast de IPv6. Las direcciones unicast globales son asignadas por IANA.

Direccionamiento físico
Ver dirección MAC.

Direcciones privadas
Parte de una dirección IP que se reserva para uso interno. Una dirección de red privada no se enruta a través de la Internet pública. En IPv4, el rango de direcciones de red privadas es de 10.0.0.0 a 10.255.255.255, 172.16.0.0 a 172.31.255.255 y 192.168.0.0 a 192.168.255.255.

Diseñador de configuración
Aplicación de Microsoft Windows que permite que el administrador configure diversos routers al mismo tiempo. El diseñador de configuración detecta automáticamente el modelo, la versión de software, el tipo de imagen, y la cantidad y el tipo de interfaces instaladas en el router que se está configurando. Importa rápidamente las listas predefinidas de colas de prioridad, las listas de acceso y los filtros a diversos archivos de configuración.

Diseño de red jerárquico
Técnica de diseño que divide la red en capas para evitar la congestión y reducir el tamaño de los dominios de fallas. El modelo de diseño jerárquico de Cisco utiliza capas de acceso, distribución y núcleo.

Disponibilidad
Condición de accesibilidad.

Dispositivo de acceso Frame Relay
Ver FRAD.

Dispositivo de extremo
Filtro en el perímetro de una red empresarial por el cual pasan los paquetes entrantes. Los dispositivos de extremo incluyen los firewalls y las DMZ. Los servicios de extremo pueden equiparse con IDS e IPS para examinar y bloquear el tráfico no deseado.

Distancia administrativa
Calificación para determinar la fiabilidad de una fuente de información de enrutamiento. En un router Cisco, la distancia administrativa se expresa por un valor numérico de 0 a 255. Cuanto mayor sea el valor, menor la calificación de fiabilidad.

Distancia factible
Ver FD.

Distancia notificada
Ver RD.

Distancia publicada
Ver AD.

Distinto costo
Se necesita ancho de banda adicional para enviar un paquete por ciertas rutas de una red. Algunas rutas pueden tener valores mayores que otras.

Divide y vencerás
Técnica de resolución de problemas para solucionar un problema de red dividiendo el problema en partes más pequeñas que son más fáciles de administrar.

DLCI
Identificador de conexión de enlace de datos.

Dirección de Capa 2, necesaria para que cada circuito virtual alcance su destino en una red de NBMA. El DLCI se almacena en el campo de direcciones de cada trama transmitida. El DLCI, en general, tiene sólo importancia local y puede ser diferente en cada extremo de un circuito virtual.

DMZ
Zona desmilitarizada.

Área de un diseño de red ubicada entre la red interna y la red externa (normalmente Internet). La DMZ es accesible para los dispositivos de Internet, como servidores Web, servidores FTP, servidores SMTP y DNS.

DNS
Sistema de nombres de dominios.

Sistema que se utiliza en Internet para convertir los nombres de los nodos de red en direcciones IP

Dominio
Parte del árbol de jerarquía de denominación que se refiere a las agrupaciones generales de redes basadas en el tipo de organización o geografía.

Dominio de administración
Información incluida en un mensaje que cada switch publica en sus puertos de enlace troncal.

Dominio de broadcast
Conjunto de dispositivos que recibe tramas de broadcast que tienen su origen en cualquiera de los dispositivos dentro del conjunto. Los dominios de broadcast generalmente están limitados por routers, dado que éstos no envían tramas de broadcast.

Dominio de colisiones
Área de la red en Ethernet donde se propagan las tramas que sufrieron una colisión. Los repetidores y los hubs tienen dominios de colisión. Los switches LAN, los puentes y los routers no.

Dominio de enrutamiento
Grupo de sistemas finales y sistemas intermedios que operan bajo el mismo conjunto de normas administrativas. Dentro de cada dominio de enrutamiento hay una o más áreas, cada una identificada de forma exclusiva mediante una dirección de área.

Dominio de fallas
Área de una red que se ve afectada cuando se produce una falla o un mal funcionamiento en un dispositivo de red. Con un diseño adecuado para la red, se minimiza el tamaño de los dominios de fallas.

Dominios de colisión
Área de la red en Ethernet donde se propagan las tramas que sufrieron una colisión. Los repetidores y los hubs tienen dominios de colisión. Los switches LAN, los puentes y los routers no.

DoS
Denegación de servicio.

Ataque de un único sistema a una red. Consiste en saturar el ancho de banda o los recursos del sistema objetivo (por ejemplo, un servidor Web) con el propósito de desactivarlo.

Dot1q
Ver 802.1q.

DRAM
Memoria dinámica de acceso aleatorio.

En un router Cisco, esta memoria de trabajo no permanente incluye la DRAM principal utilizada para reservar tablas de enrutamiento y la configuración en ejecución, y la DRAM compartida que se utiliza para la compatibilidad con los búferes de paquetes.

DROther
Cualquier router de una red de OSPF que no sea DR o BDR.

DS0
Señal digital de nivel 0.

Especificación de entramado que se usa para transmitir señales digitales a través de un solo canal a 64 kbps en una instalación T1.

DS1
Capa 1 de la señal digital.

Especificación de entramado utilizada en la transmisión de señales digitales a 1544 Mbps en una instalación T1 (en los Estados Unidos) o a 2108 Mbps en una instalación E1 (en Europa).

DS3
Señal digital de nivel 3.

Especificación de entramado que se usa para transmitir señales digitales a 44 736 Mbps en una instalación T3.

DSCP

Punto de código de servicios diferenciados.

Campo de un paquete IP que permite asignar distintos niveles de servicio al tráfico de red. El DSCP puede ser asignado por el router o por el switch. Los primeros seis bits del byte de ToS en el encabezado constituyen el DSCP.

DSL

Servicio de red pública que proporciona un gran ancho de banda a distancias limitadas a través del cableado de cobre de las líneas telefónicas convencionales que se tienden entre el CPE y el DSLAM de un SP. El DSL incorpora tecnología que permite que los dispositivos se conecten inmediatamente a Internet cuando se los enciende. Es una tecnología de transmisión de capas físicas similar a las tecnologías de marcado telefónico, de cable o inalámbricas.

DSU

Unidad de servicio de datos.

Dispositivo de transmisión digital que se usa en la transmisión digital que adapta la interfaz física de un dispositivo DTE a una instalación de transmisión, por ejemplo, T1 y E1. La DSU también es responsable de funciones tales como la temporización de señal. A menudo se denomina, en forma conjunta con CSU, CSU/DSU.

DTE

Equipo terminal de datos.

Conexión física al usuario final en un entorno de expansión EIA. El DTE sirve como destino u origen de datos, o como ambos. Se conecta a una red de datos a través de un dispositivo DCE (por ejemplo, un módem) y, por lo general, usa señales de temporización generadas por el DCE. El DTE incluye dispositivos como, por ejemplo, computadoras, traductores de protocolo y multiplexores.

DUAL

Algoritmo de actualización difuso.

Proceso matemático utilizado en EIGRP, que permite operaciones sin bucles, en todo momento, durante el cálculo de rutas. DUAL permite que los routers involucrados en un cambio de topología se sincronicen al mismo tiempo, sin involucrar a los routers que no se ven afectados por el cambio.

Duración de prefijo

Identifica la cantidad de bits utilizados en la red.

La duración de prefijo también se denomina prefijo de red.

DVMRP

Protocolo de enrutamiento multicast de vector distancia.

Protocolo de gateway de internetwork, basado en gran parte en RIP, que implementa un esquema IP multicast de modo denso típico. El DVMRP usa IGMP para intercambiar datagramas de enrutamiento con sus vecinos.

DWDM

Multiplexación por división de longitud de onda densa.

Proceso que asigna señales ópticas entrantes a frecuencias o longitudes de onda de luz específicas. El DWDM puede amplificar estas longitudes de onda para potenciar la intensidad de la señal. Puede multiplexar más de 80 longitudes de onda o canales de datos diferentes en una única porción de fibra. Cada canal puede transportar una señal multiplexada a 2,5 Gbps.

E1
Esquema de transmisión digital de área amplia que se usa predominantemente en Europa y transporta datos a una velocidad de 2048 Mbps. Las líneas E1 para uso privado pueden arrendarse a las compañías telefónicas.

E1 fraccional
Parte de una conexión E1 de gran ancho de banda ofrecida a un cliente por un proveedor de servicios.

E2
Ruta fuera del dominio de enrutamiento OSPF, redistribuida en OSPF.

E3
Esquema de transmisión digital de área amplia que se usa predominantemente en Europa y transporta datos a una velocidad de 34,368 Mbps. Las líneas E3 para uso privado se pueden arrendar a las empresas telefónicas.

ECNM
Modelo de red empresarial compuesta.

Diseño de red de Cisco que divide la red en componentes funcionales, mientras mantiene el concepto de capas de acceso, distribución y núcleo. Los componentes funcionales son: Campus empresarial, Extremo empresarial y Extremo del proveedor de servicios.

EGP
Protocolo de gateway exterior.

Estándares para intercambiar información de enrutamiento entre sistemas autónomos. El EGP es un protocolo obsoleto que fue reemplazado por el protocolo de border gateway.

EIGRP
Protocolo de enrutamiento de gateway interior mejorado.

Protocolo de enrutamiento patentado de Cisco que combina los estándares de protocolo de enrutamiento de vector distancia y los de protocolo de enrutamiento del estado de enlace. EIGRP utiliza el algoritmo DUAL para determinar el enrutamiento.

El EIGRP también se denomina IGRP mejorado.

EIR
Velocidad de información excesiva.

Velocidad promedio por encima de la CIR que puede admitir un VC cuando no hay congestión en la red.

Elegible para descarte
Ver DE.

EMI
Interferencia electromagnética.

Perturbación en un circuito electrónico causada por una fuente eléctrica externa.

Empresa
Corporación, negocio o entidad que utiliza computadoras en un entorno de red. Normalmente, hace referencia a grandes empresas u organizaciones con redes complejas.

Encabezado
Información de control que se coloca antes de los datos al encapsular esos datos para su transmisión por la red. Las direcciones IP del emisor y del destinatario son ejemplos de la información que se incluye en el encabezado.

Encabezado de autenticación
Ver AH.

Encapsulación
Transmisión de un protocolo de red dentro de otro. El proceso denominado tunneling es la base de diversos sistemas de seguridad IP, incluido IPsec, utilizado en las VPN.

Encapsulación de enrutamiento genérico
Ver GRE.

Encriptación
Aplicación de un algoritmo específico que protege los datos pues codifica la información cuando se la envía y descodificándola cuando se la entrega.

Enfoque descendente
Método de prueba de red diseñado para admitir determinadas aplicaciones y requerimientos de servicio de redes. Cuando se completa un diseño, se realiza una prueba piloto usando el enfoque descendente para garantizar que el nuevo diseño funcione como se espera, antes de su implementación.

Enlace
Canal de comunicaciones de red que incluye un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

Un enlace también se conoce como línea o enlace de transmisión.

Enlace de acceso
Conexión entre un DTE, por ejemplo, un router, y el punto de presencia más cercano de un proveedor de servicios mediante un DCE, por ejemplo, un módem en una red Frame Relay.

Enlace de ruta virtual
Ver VPL.

Enlace Inter-Switch
Ver ISL.

Enlace redundante
Conexión secundaria entre los dispositivos de red para asegurar la disponibilidad de red si falla el enlace principal.

Enlace troncal
Enlace punto a punto que conecta un switch a otro switch, un router o un servidor. El enlace troncal transporta tráfico por múltiples VLAN por el mismo enlace. Las VLAN son multiplexadas por el enlace con un protocolo de enlace troncal.

Enrutamiento
Proceso cuya meta es encontrar una ruta hacia un host de destino. El enrutamiento es complejo en redes de gran tamaño debido a los destinos intermedios que un paquete puede tener que atravesar antes de llegar al host de destino final.

Enrutamiento con clase
Selección de una ruta de la red sin incluir información sobre la máscara de subred. El enrutamiento con clase no es compatible con las máscaras de subred de longitud variable.

Enrutamiento de la ruta libre más corta
Ver SPR.

Enrutamiento dentro del área
Transferencia de datos dentro de un área lógica cuando el origen y el destino están en la misma área.

Enrutamiento dinámico
Proceso que consiste en buscar una ruta que se ajuste automáticamente a los cambios de tráfico o de topología de la red.

El enrutamiento dinámico también se conoce como enrutamiento adaptable.

Enrutamiento entre áreas
Transferencia de datos entre dos o más áreas lógicas.

Enrutamiento entre dominios sin clase
Ver CIDR.

Enrutamiento jerárquico
Transferencia de datos en un sistema que asigna direcciones de red según la función o la posición del host o del dispositivo de red.

Enrutamiento multiprotocolo de etiquetas
Ver MPLS.

Enrutamiento por políticas
Esquema de enrutamiento que envía paquetes a interfaces específicas de una red según las políticas configuradas a nivel de usuario. Un ejemplo del enrutamiento por políticas es que podría especificar que el tráfico enviado desde una red determinada debe enviarse desde una interfaz, mientras que el resto del tráfico debe enviarse desde otra interfaz.

Enrutamiento sin clase
Función de un protocolo donde la máscara de subred se envía con todos los paquetes de actualización de enrutamiento. Los protocolos de enrutamiento sin clase incluyen RIPv2, EIGRP y OSPF.

Entrante
Una de dos direcciones en las que viaja un paquete en una red a través de una interfaz. Un paquete entrante ingresa en un dispositivo.

Envenenamiento de rutas
Configuración de la métrica para ruta en 16 a fin de detener el tráfico en la ruta. El RIP envía una actualización generada por eventos de forma inmediata, lo cual envenena la ruta.

Envenenamiento en reversa
Actualización de enrutamiento que indica que una red o subred es inalcanzable, en lugar de dar a entender que una red es inalcanzable al no incluirla en las actualizaciones. Las actualizaciones de

envenenamiento en reversa se envían para dejar sin efecto los grandes routing loops. La implementación del IGRP de Cisco usa actualizaciones de envenenamiento en reversa.

Envío rápido
Método de conmutación por corte mediante el cual el switch envía la trama antes de que se la haya recibido por completo. Mediante el método de envío rápido, el switch envía la trama al puerto de destino inmediatamente después de leer la dirección MAC de destino. El switch no calcula ni comprueba el valor de CRC. Este método tiene la latencia más baja, pero también puede enviar fragmentos de colisión y tramas dañadas. Este método de conmutación funciona mejor en una red estable con pocos errores.

EOT
Fin de la transmisión.

Carácter que denota que ha terminado la transferencia de datos.

Equipo de comunicación de datos
Ver DCE.

Equipo local del cliente
Ver CPE.

Equipo terminal de datos
Ver DTE.

Escalabilidad
Capacidad de un diseño de red para desarrollar la inclusión de nuevos grupos de usuarios y sitios remotos. Un diseño de red escalable debe ser compatible con nuevas aplicaciones sin afectar el nivel de servicio proporcionado a los usuarios existentes.

Escucha
Uno de los cuatro estados por los que pasa un puerto cuando se enciende un switch en una red STP. El switch escucha los BPDU desde los switches vecinos.

ESP
Contenido de seguridad encapsulado.

Protocolo de seguridad que encapsula los datos que se deben proteger. ESP proporciona un marco para la encriptación, la autenticación y la protección de datos. El ESP ofrece servicios de privacidad de datos, autenticación de datos opcionales y servicios sin repetición.

Espera
Colocación de un router en un estado en el que no publica ni acepta rutas por un período específico de tiempo, que se conoce como período de espera. La espera se usa para eliminar la información defectuosa acerca de una ruta de todos los routers de la red. Suele colocarse en espera una ruta cuando falla un enlace de esa ruta.

Estándar abierto
Protocolo o regla disponible para el público, que puede aplicarse a una red. Un estándar abierto no es propiedad privada.

Estándar de cifrado de datos
Ver DES.

Estándar de cifrado triple de datos
Ver 3DES.

Estándar de encriptación avanzada
Ver AES.

Estándar de hecho
Formato, idioma o protocolo que se convierte en estándar porque se populariza. En contraste, un estándar de jure es el que existe porque fue aprobado por un organismo oficial de homologación.

Estrella
Estructura en la cual los dispositivos de una red se conectan a un switch central común mediante enlaces punto a punto. La topología en estrella es la topología física usada más comúnmente para LAN Ethernet.

Estrella extendida
Topología en estrella que se expande, a fin de incluir dispositivos de red adicionales.

EtherChannel
EtherChannel permite combinar diversos vínculos Ethernet físicos en un canal lógico. Esto permite el balanceo de carga del tráfico entre los enlaces del canal, además de proporcionar redundancia en caso de que falle un enlace del canal o varios. EtherChannel es compatible con los puertos LAN de Capa 2 o Capa 3.

Ethernet
Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Una red Ethernet utiliza el método de Acceso múltiple con detección de portadora y detección de colisiones y se ejecuta con tipos de cable de 10 Mbps o más. Ethernet es similar al conjunto de estándares IEEE 802.3.

Etiquetado de trama
Método utilizado por los switches Catalyst de Cisco para identificar a qué VLAN pertenece una trama. Cuando una trama ingresa al switch, se la encapsula con un encabezado que la etiqueta con una identificación de la VLAN.

EUI-64
Dirección extendida universal de 64 identificadores.

Formato de dirección de IPv6 creado mediante una interfaz de la dirección MAC, que tiene una longitud de 48 bits, y mediante el agregado de otra cadena hexadecimal de 16 bits, FFFE, entre la OUI (los primeros 24 bits) y el número de serie único (últimos 24 bits) de la dirección MAC. Para garantizar que la dirección elegida provenga de una dirección MAC de Ethernet, el séptimo bit del byte de orden superior se establece en 1 para indicar que la dirección de 48 bits es única.

Extranet
Red que proporciona acceso a información u operaciones de una organización a proveedores, fabricantes, socios, clientes u otras empresas. La extranet es una red privada que utiliza protocolos de Internet y el sistema de telecomunicación público para compartir recursos internos. Puede considerarse una extensión de una intranet.

Facilidad de administración
Capacidad de administración de un sistema.

Factor de forma
Tamaño y forma físicos de los componentes informáticos. Los componentes que comparten el mismo factor de forma son intercambiables físicamente.

Fast Ethernet
Especificación de Ethernet 100BaseT que ofrece una velocidad 10 veces mayor que la especificación Ethernet 10BASE-T estándar, mientras conserva cualidades, por ejemplo, el formato de las tramas, los mecanismos de MAC y la MTU. Se basa en una extensión de la especificación IEEE 802.3.

FCS
Secuencia de verificación de trama.

Caracteres que se agregan a una trama con el fin de controlar los errores. Se usa en HDLC, Frame Relay y otros protocolos de la capa de enlace de datos.

FD
Distancia factible.

Mejor métrica de EIGRP para la ruta desde el router hasta el destino.

FECN
Notificación explícita de congestión hacia adelante.

Señal en una red Frame Relay para informar a DTE que está recibiendo la trama sobre una congestión en la ruta desde el origen hasta el destino. El DTE que recibe la señal de FECN puede solicitar que se lleve a cabo una acción de control de flujo por parte de los protocolos de nivel superior.

Fiabilidad
Relación entre los mensajes de actividad esperados y recibidos de un enlace. Si la relación entre los mensajes de actividad es alta, la línea es confiable. La fiabilidad se utiliza como métrica de enrutamiento.

Filtrado de tráfico
Controla el tráfico en distintos segmentos de la red. El filtrado de tráfico es el proceso que consiste en analizar los contenidos de un paquete para determinar si éste debe ser permitido o bloqueado.

Filtro
Proceso o dispositivo que evalúa el tráfico de red en busca de determinadas características, como ser: dirección de origen, dirección de destino o protocolo, y determina si ese tráfico se debe enviar o descartar basándose en los criterios establecidos.

Fin de la transmisión
Ver EOT.

Firewall (FW)
Uno o más routers o servidores de acceso designados como búfer entre cualquier red pública conectada y una red privada. El router firewall usa listas de acceso y otros métodos para garantizar la seguridad de la red privada.

Flooding
Técnica utilizada por los switches para transmitir tráfico que se recibe en una interfaz a todas las demás interfaces del dispositivo, excepto a la interfaz en la que se recibió originalmente la información.

Fluctuación de fase
Distorsión analógica de la línea de comunicación. La fluctuación de fase puede tener su causa en la variación de una señal desde las posiciones de temporización de referencia, en la congestión de la red o en cambios de rutas. Puede provocar la pérdida de datos, especialmente a altas velocidades.

Formato IETF
Grupo de trabajo compuesto por alrededor de 80 grupos que tienen la responsabilidad de desarrollar estándares de Internet. El IETF es parte de la Sociedad de Internet o ISOC.

FRAD
Dispositivo de acceso Frame Relay.

Dispositivo de red que proporciona una conexión entre una LAN y una WAN Frame Relay. Un FRAD agrega y elimina los encabezados y la información final de los paquetes.

Fragmentación
Proceso por el cual un paquete se divide en unidades más pequeñas al realizar la transmisión a través de un medio de red que no puede admitir el tamaño del paquete.

Fragmento
Parte de un paquete que se ha dividido en unidades más pequeñas.

Frame Relay
Estándar de conmutación industrial aplicado a WAN que funciona en la capa física y en la capa de enlace de datos del modelo de referencia de OSI. Frame Relay administra diversos circuitos virtuales mediante la encapsulación de HDLC entre los dispositivos conectados. Es más eficaz que el protocolo X.25 al que reemplazó.

FRAS
Soporte de acceso Frame Relay.

Característica del software IOS de Cisco que permite que los dispositivos IBM de SDLC, Token Ring, Ethernet y Frame Relay se conecten a otros dispositivos IBM a través de una red Frame Relay.

FTP
Protocolo de transferencia de archivos.

Conjunto de estándares definidos en RFC 959 para la transferencia de archivos entre nodos de la red. Por lo general, el FTP se utiliza para transferir páginas Web y descargar programas y otros archivos a una computadora.

Fuente de energía ininterrumpible
Ver UPS.

Fuera de banda
Transmisión que usa frecuencias o canales fuera de las frecuencias o canales que se usan normalmente para la transferencia de información. La señalización fuera de banda se usa a menudo para informar acerca de la existencia de errores en situaciones en las que la señalización dentro de la banda se puede ver afectada por los problemas que la red pueda estar experimentando.

Garantía
Garantía de que un producto o servicio está libre de defectos y funciona tal como se lo publicitó. La garantía es limitada en duración y en los servicios otorgados.

Gateway
Dispositivo que lleva a cabo la conversión de información de un stack de protocolos a otro en la capa de aplicación. Un ejemplo de un gateway es el dispositivo que conecta un PSTN tradicional o teléfono análogo a una red IP en VoIP.

Gateway de borde
Router que se comunica con routers de otros sistemas autónomos.

Gateway de último recurso
En una ruta empresarial, parada final de los paquetes que no presentan coincidencias. La información sobre los paquetes aparece en las tablas de enrutamiento de todos los routers.

Gateway predeterminado
Ruta de un paquete de red utilizada de forma predeterminada, o como último recurso, cuando los hosts de destino no figuran en la tabla de enrutamiento.

GDP
Protocolo de descubrimiento de gateway.

Estándar de Cisco que permite que un host detecte de forma dinámica el arribo de un nuevo router y que, además, determine cuándo se desconecta. El GDP se basa en UDP.

Gigabit Ethernet
Ancho de banda de transmisión de datos a 1000 Mbps en una LAN. Gigabit Ethernet es el estándar de Ethernet de alta velocidad, aprobado por el comité de estándares IEEE 802.3z en 1996.

Gigante
Trama Ethernet de una red que se etiquetó como demasiado extensa. Los gigantes se descartan y se registran como errores.

GMT
Hora del Meridiano de Greenwich.

Huso horario ubicado a 0 grados de longitud, referencia para establecer la hora de todos los demás husos.

Granjas de servidores
Conjunto de servidores localizados en una instalación central y administrados por el grupo central a fin de satisfacer las necesidades de servidor de las organizaciones. Por lo general, una granja de servidores tiene hardware principal y de respaldo para balanceo de carga, redundancia y tolerancia a fallas. La arquitectura de las granjas de servidores proporciona el mantenimiento y la operación de los servidores.

GRE
Encapsulación de enrutamiento genérico.

Protocolo de tunneling de Cisco que se utiliza para encapsular diferentes protocolos en un protocolo estándar de Internet a fin de transferirlo.

Grupo de direcciones de protocolo de Internet
Ver grupo de direcciones IP.

Grupo de direcciones IP
Grupo de direcciones de protocolo de Internet.

Rango de direcciones IP registradas para utilizarse con NAT.

Grupo de trabajo de ingeniería de Internet
Ver IETF.

Hash
Algoritmo de encriptación unidireccional que comienza con un mensaje de entrada de longitud arbitraria y produce texto de salida único de longitud fija.

HCC
Conexión cruzada horizontal.

Armario para el cableado en el que el cableado horizontal se conecta a un panel de conexión que se conecta a través de cableado backbone a la instalación de distribución principal.

HDLC
Control de enlace de datos de alto nivel.

Protocolo de capa de enlace de datos síncrono, orientado a bits, desarrollado por ISO. HDLC especifica un método para encapsular datos en enlaces seriales síncronos usando caracteres de trama y checksums.

Hexadecimal
Sistema numérico Base 16 Representación numérica que usa los dígitos 0 a 9, con su significado habitual, y las letras de la A a la F para representar dígitos hexadecimales con valores de 10 a 15. El dígito ubicado más a la derecha cuenta unos, el siguiente cuenta múltiplos de 16, por ejemplo, 16^2=256.

HMAC
Algoritmo que usa funciones criptográficas de hash para encriptar el código. Puede utilizarse el HMAC con cualquier función criptográfica de hash iterativa, como MD5 o SHA-1, en combinación con una clave secreta compartida.

HMAC-MD5
Código de autenticación de mensajes de hash: message digest 5.

Algoritmo que utiliza una función criptográfica de hash específica llamada MD5, con una clave secreta. El resultado es una cadena de hash de 128 bits que puede utilizarse para verificar la integridad de los datos y la autenticidad de un mensaje de forma simultánea.

HMAC-SHA-1
Código de autenticación de mensajes de hash: Algoritmo de hash seguro 1.

Algoritmo que utiliza una función criptográfica de hash específica llamada SHA-1, con una clave secreta. El resultado es una cadena de hash de 160 bits que puede utilizarse para verificar la integridad de los datos y la autenticidad de un mensaje de forma simultánea.

Hora del Meridiano de Greenwich
Ver GMT.

Horizonte dividido
Técnica de enrutamiento que controla la formación de bucles e impide que la información salga de la interfaz del router a través de la misma interfaz por la que fue recibida.

Hot Standby Router Protocol
Ver HSRP.

HSRP
Hot Standby Router Protocol.

Estándar que proporciona la posibilidad de comunicación en una internetwork si el router predeterminado no se encuentra disponible. El HSRP suministra alta disponibilidad de red y cambios transparentes en la topología de la red.

HSSI
Interfaz serial de alta velocidad.

Protocolo que establece los códigos y parámetros eléctricos que el router y la CSU/DSU utilizan para comunicarse entre sí.

HTTP
Protocolo de transferencia de hipertexto.

Estándar utilizado para transferir o comunicar información en la World Wide Web. El HTTP es un protocolo de comunicación que establece una conexión de solicitud/respuesta en Internet.

HWIC
Tarjeta de interfaz WAN de alta velocidad.

Módulo opcional para una serie de routers Cisco que proporciona conectividad WAN de alta velocidad.

IANA
Agencia de asignación de números de Internet.

Entidad que ejerce control sobre los números del sistema autónomo y que sirve como registro de las direcciones IP y los números de protocolo.

ICMP
Protocolo de mensajes de control de Internet (Internet Control Message Protocol).

Estándar para la resolución de problemas y la verificación de capas de red. El ICMP brinda la posibilidad de declarar mensajes de diagnóstico y de error. El comando ping es parte de la utilidad de ICMP.

ID de área
Identificación del área de OSPF a la que pertenece la red.

ID de clave
Identificación del código utilizado entre dispositivos.

ID de la VLAN
Ver VID.

ID del router
Dirección de IP determinada por un valor configurado con el comando `router-id`, un valor de la dirección de IP más alta configurada en una interfaz loopback, o un valor de la dirección de IP más alta en cualquier interfaz física.

ID de puente
Ver BID.

Identificador de conexión de enlace de datos
Ver DLCI.

Identificador de conjunto de servicios
Ver SSID.

Identificador exclusivo de organización
Ver OUI.

IDF
Instalación de distribución intermedia.

Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF tiene una trama con una conexión cruzada desde los medios de cable del usuario hasta los circuitos de línea de usuario y puede servir como punto de distribución de cables con múltiples pares desde la trama de distribución principal. El IDF depende del MDF.

IDS
Sistema de detección de intrusión.

Combinación de un sensor, una consola y un motor central en un único dispositivo instalado en una red para protegerla contra los ataques que un firewall convencional quizá no detecte. El IDS inspecciona toda la actividad de red entrante y saliente e identifica los patrones sospechosos que pueden indicar un ataque al sistema o a la red. El IDS se configura para que envíe una alarma a los administradores de la red cuando se detecta dicho ataque.

IEEE
Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares LAN del IEEE son los estándares de LAN predominantes en el mundo actual.

IEEE 802.1q
Estándar de IEEE diseñado para permitir el tráfico entre LAN virtuales. El estándar 802.1q de IEEE utiliza un mecanismo de etiquetado interno que agrega un campo de etiqueta de cuatro bytes en la trama Ethernet original, entre la dirección de origen y los campos de tipo/longitud. Dado que se altera la trama, el dispositivo de enlace troncal vuelve a calcular la secuencia de verificación de trama en la trama modificada.

IETF
Grupo de trabajo compuesto por alrededor de 80 grupos que tienen la responsabilidad de desarrollar estándares de Internet. El IETF es parte de la Sociedad de Internet o ISOC.

IGMP
Protocolo de administración de grupos de Internet.

Estándar utilizado por los host IP para informar al router multicast adyacente su pertenencia a los grupos de multicast. Puede utilizarse el IGMP para tener acceso a video y juegos en línea de forma más eficiente.

IGP
Protocolo de gateway interior.

Estándar que se usa para intercambiar información de enrutamiento dentro de un sistema autónomo. Entre los ejemplos de protocolos IGP Internet comunes, se incluyen EIGRP, OSPF y RIP.

Igual costo
Técnica de distribución de paquetes admitida por EIGRP para evitar la sobrecarga de una ruta de red.

IKE
Intercambio de claves de Internet.

Protocolo híbrido obtenido a partir de los estándares ISAKMP y Oakley, que proporciona servicios utilitarios para IPSec que incluyen la autenticación de los pares de IPSec, la negociación de las asociaciones de seguridad IKE e IPSec y el establecimiento de claves para los algoritmos de encriptación utilizados por IPSec.

Indicador de intensidad de la señal del receptor
Ver RSSI.

Inspección de paquetes con estado
Ver SPI.

Instalación de distribución intermedia
Ver IDF.

Instalación de distribución principal (MDF)
Instalación de distribución principal.

Recinto de comunicación primaria de un edificio. La MDF es el punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, los hubs y los routers. Se utiliza para conectar las líneas públicas o privadas que ingresan al edificio con las redes internas.

Instalación piloto
Pequeña implementación de una nueva tecnología de red que se utiliza para evaluar cómo cumple la tecnología los objetivos de diseño.

Instituto de ingenieros eléctricos y electrónicos
Ver IEEE.

Integridad de datos
Proceso, estrategia y tecnología que garantiza que los datos no cambien desde su creación hasta su recepción.

Inter-VLAN
Enrutamiento dentro de una LAN virtual. Es necesario configurar los switches y los routers de forma específica.

Intercambiable en caliente
Capacidad de un componente para ser instalado o desconectado sin necesidad de desconectar la alimentación en primer lugar. La instalación o la desconexión de un componente intercambiable en caliente no afecta el funcionamiento de los demás componentes de un dispositivo.

Intercambio de claves
Método para que dos pares establezcan una clave secreta compartida, que sólo ellos puedan reconocer, al comunicarse por un canal no seguro.

Intercambio de claves de Internet
Ver IKE.

Intercambio privado de ramas
Ver PBX.

Interfaz
1) Conexión entre dos sistemas o dispositivos. 2) En la terminología de enrutamiento, una conexión de red. 3) En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4) El límite entre capas adyacentes del modelo OSI.

Interfaz de administración local
Ver LMI.

Interfaz de línea de comandos
Ver CLI.

Interfaz de salida
Ubicación en un router que deben atravesar los datos para acercarse al destino.

Interfaz loopback
Conexión entre dispositivos que comparten el mismo tipo de enrutamiento.

Interfaz Null0
El EIGRP instala un resumen de ruta Null0 en la tabla de enrutamiento para cada ruta principal. La interfaz Null0 indica que no se trata de una ruta real, sino de un resumen generado para la publicación.

Interfaz serial de alta velocidad
Ver HSSI.

Interferencia electromagnética
Ver EMI.

Interferencia radioeléctrica
Ver RFI.

Internetwork
Conjunto de redes interconectadas por routers y otros dispositivos que funcionan como una sola red.

Intervalo activo
Período de tiempo durante el cual el cliente espera antes de enviar un mensaje de actividad en una conexión TCP.

Intervalo de saludo
Período de tiempo, en segundos, durante el cual el router mantiene un paquete de saludo de un vecino.

Intervalo muerto
Período de tiempo, en segundos, que espera un router para escuchar un saludo de parte de un vecino antes de declararlo desconectado.

Intranet
Redes a las que pueden acceder los usuarios internos de una organización. La intranet se utiliza para compartir información interna y recursos informáticos.

Inverso
Que tiene el efecto opuesto.

IP multicast
Multicast de protocolo de Internet.

Técnica de enrutamiento donde un paquete se envía a un grupo de multicast que se identifica mediante una sola dirección IP de destino. IP multicast ahorra ancho de banda de la red porque los paquetes se transmiten como flujo por el backbone y sólo se dividen para ser enviados a las estaciones de destino por el router al final de la ruta.

IP móvil
Protocolo de Internet móvil.

Estándar de IETF para IPv4 e IPv6 que permite a un dispositivo móvil trasladarse sin interrumpir la conexión. La movilidad es una función de IPv6.

IPCP
Protocolo de control de IP.

Estándar para establecer y configurar IP por PPP. IPCP es responsable de la configuración, la activación y la desactivación de los módulos de protocolo IP a ambos extremos del enlace punto a punto.

IPS
Sistema de prevención de intrusión.

Dispositivo activo en la ruta de tráfico que monitorea el tráfico de red y permite o rechaza los flujos y los paquetes dirigidos hacia la red. Todo el tráfico pasa a través de un IPS para ser inspeccionado. Cuando el IPS detecta tráfico malicioso, envía una alerta a la estación de administración y bloquea el tráfico malicioso de inmediato. El IPS evita los ataques de manera proactiva mediante el bloqueo del tráfico malicioso original y subsiguiente.

IPSec
Seguridad de IP.

Marco de estándares abiertos que proporciona confidencialidad de datos, integridad de datos y autenticación de datos entre los pares participantes. La IPSec proporciona servicios de seguridad en la capa IP. Utiliza IKE para administrar la negociación de protocolos y algoritmos según las políticas locales y para generar las claves de encriptación y autenticación que debe utilizar IPSec. IPSec puede proteger uno o más flujos de datos entre un par de hosts, entre un par de gateways de seguridad o entre un gateway de seguridad y un host.

IPv4
Protocolo de Internet versión 4.

Estándar actual de capas de red para las internetworks de conmutación de paquetes. La dirección IP de IPv4 es de 32 bits.

IPv6
Protocolo de Internet versión 6.

Estándar de capas de red para las internetworks de conmutación de paquetes. IPv6 es el sucesor de IPv4 para uso general en Internet.

IPXCP
Protocolo de control de intercambio de paquetes de internetwork.

Estándar que establece y configura IPX a través de PPP.

IS-IS
Sistema intermedio a sistema intermedio.

Sistema para el enrutamiento jerárquico de estado de enlace de OSI basado en el enrutamiento DECnet de Fase V. Los routers intercambian información según una métrica individual para determinar la topología de la red.

ISL
Enlace Inter-Switch.

Protocolo de Cisco para el etiquetado de tramas en una red IEEE 802.1q.

ITU-T
Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones.

Organización internacional que desarrolla estándares de comunicación.

Anteriormente, la ITU-T se conocía como Comité Internacional Telegráfico y Telefónico.

IVR
Respuesta de voz interactiva.

Un sistema que proporciona información en forma de mensajes grabados por líneas telefónicas en respuesta a información ingresada por el usuario en forma de palabras o señales de multifrecuencia de dos tonos. Los ejemplos de IVR incluyen la posibilidad de consultar el balance de una cuenta bancaria por teléfono.

Jabber
1) Condición de error en la que un dispositivo de red transmite continuamente datos aleatorios, sin sentido, a la red. 2) Paquete de datos que supera la longitud prescrita en el estándar IEEE 802.3.

Jerarquía digital síncrona
Ver SDH.

L2TP
Estándar de tunneling de PPP mediante una red pública. L2TP proporciona un método de implementación de redes privadas de marcado telefónico virtual basado en L2F y protocolos de tunneling punto a punto. L2TP es un protocolo de seguimiento estándar del grupo de trabajo de ingeniería de Internet, definido en RFC 2661.

LAN
Red de área local.

Sistema de transferencia de datos de alta velocidad y bajo porcentaje de errores, que abarca un área geográfica reducida. Las LAN conectan estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos que se encuentran en un mismo edificio u otras áreas geográficas limitadas. Los estándares de LAN especifican el cableado y la señalización en las capas física y de enlace de datos del modelo de referencia OSI. Entre los ejemplos de tecnologías LAN se incluyen Ethernet, FDDI y Token Ring.

LAN dedicada
Red de área local inalámbrica dedicada.

Segmento de red que se asigna a un solo dispositivo. La tecnología LAN dedicada se utiliza en topologías de red LAN conmutadas.

LAN inalámbrica
Ver WLAN.

LAP
Puntos de acceso livianos.

Puntos de acceso utilizados en la arquitectura de red inalámbrica unificada de Cisco. Los LAP dependen de un controlador de LAN inalámbrica de Cisco para obtener información de configuración y seguridad.

Latencia
1) Retardo entre el momento en el que un dispositivo recibe una trama y el momento en el que la trama sale desde el puerto de destino. 2) La latencia de datos es el tiempo que transcurre entre una consulta y el momento en el que se muestran los resultados en la pantalla.

LCP
Protocolo de control de enlace.

Estándar que establece, configura y prueba las conexiones de enlace de datos que usa PPP. El LCP verifica la identidad del dispositivo vinculado, determina el tamaño aceptable de los paquetes, busca errores y puede interrumpir la conexión del enlace si éste supera los requisitos.

libre de fragmentos
Parte de un paquete que se ha dividido en unidades más pequeñas.

Límite con clase
Designación de subredes como red de una única clase, A, B o C, por parte de protocolos como RIP y EIGRP.

Límite de la red
Lugar donde se produce la sumarización de rutas en un router de borde.

Línea arrendada
Ancho de banda de una línea de comunicación reservada por una empresa de telecomunicaciones para uso privado de un cliente. Una línea arrendada es un tipo de línea dedicada.

Línea de acceso telefónico
Circuito de comunicaciones que se establece mediante una conexión de circuito conmutada usando la red de la compañía telefónica.

Línea de base
Expresión cuantitativa de los costos, las programaciones y los requisitos técnicos planificados para un proyecto definido. Se establece una línea de base para describir el estado “normal” del rendimiento de una red o de un sistema de computación. Esto permite comparar el estado con la línea de base en cualquier momento para medir la variación con respecto a las condiciones de funcionamiento “normal”.

Línea de base de red
Proceso que implica el monitoreo del rendimiento y el funcionamiento de la red durante cierto período de tiempo para crear un punto de referencia para futuras evaluaciones de la red. La línea de base de red es utilizada por los administradores de red para monitorear la red y resolver problemas, en caso de que los haya.

Línea de suscriptor digital
Ver DSL.

Línea dedicada
Ancho de banda de una línea de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse cuando se requiere transmitir.

Líneas arrendadas
Ancho de banda de una línea de comunicación reservada por una empresa de telecomunicaciones para uso privado de un cliente. Una línea arrendada es un tipo de línea dedicada.

Lista de materiales
Ver BOM.

Lista de servidores de acceso nombrada
Ver NACL.

Listas de control de acceso (ACL, Access control lists)
Lista de control de acceso.

Lista generada por un dispositivo de red, como un router, para administrar el acceso desde el router o hacia él para diversos servicios. Por ejemplo, la ACL puede ser útil para impedir que los paquetes con cierta dirección IP o protocolo salgan de determinada interfaz del router.

Llamada de procedimiento remoto
Ver RPC.

LLQ
Colas de baja latencia.

Lista ordenada de prioridad estricta que permite que los datos sensibles a las demoras, como el tráfico de voz, se quiten de la secuencia y se envíen primero. Los paquetes de voz se envían a la parte de la cola de prioridad que tiene una asignación fija de ancho de banda, y se los procesa en primer lugar. Un paquete de datos ingresa al sistema de CBWFQ directamente, y se le asigna una prioridad para determinar cómo se tratan los datos. Las LLQ proporcionan colas de prioridad estricta a CBWFQ.

LMI
Interfaz de administración local.

Estándar que mejora la especificación básica de Frame Relay. La LMI incluye compatibilidad con direccionamiento global, actividad, multicast y mecanismos de estado.

LSA
Publicación de estado de enlace.

Paquete de broadcast utilizado por un protocolo de estado de enlace. La LSA contiene información sobre vecinos y costos de rutas. Los routers receptores la usan para mantener tablas de enrutamiento.

También se conoce la LSA como paquete de estado de enlace.

LWAPP
Protocolo de punto de acceso liviano.

LWAPP es un estándar de protocolo en versión preliminar que define cómo se comunican los puntos de acceso liviano con una inteligencia centralizada de WLAN. Se utiliza para administrar la seguridad, la movilidad, la calidad de servicio y otras funciones esenciales para el funcionamiento de WLAN en toda una empresa inalámbrica.

Malla
Topología de la red en la que los dispositivos se organizan de forma segmentada con interconexiones ubicadas estratégicamente entre los nodos de red.

Malla completa
Topología de red en la que cada dispositivo se conecta con todos los demás mediante un circuito físico o virtual. La malla completa proporciona redundancia en la funcionalidad de la red. Por lo general, se reserva para backbones de red, debido al alto costo de implementación.

Malla parcial
Red en la que los dispositivos están organizados en una topología de malla con nodos de red organizados en malla completa, y nodos de red conectados con uno o dos nodos de la red. Una malla parcial no suministra el nivel de redundancia de la topología de malla completa, pero su implementación es menos costosa. Se usan generalmente en las redes periféricas que se conectan a un backbone de malla completa.

Mantenimiento proactivo
Método para que el administrador de red asegure el tiempo de actividad mediante la supervisión de la funcionalidad de la red y la aplicación de medidas correctivas inmediatas. El mantenimiento proactivo se lleva a cabo regularmente para detectar debilidades antes de que se produzca un error crítico que podría hacer que la red dejara de funcionar.

Mapa de ruta
Método para controlar y modificar la información de enrutamiento en una red. Un mapa de ruta es una lista de acceso compleja que permite que algunas condiciones se verifiquen en la ruta en cuestión. Si las condiciones coinciden, se pueden tomar tomar medidas para modificar la ruta.

Máscara de dirección
Combinación de bits utilizada para identificar qué parte de una dirección se refiere a la red o subred y qué parte se refiere al host.

Máscara de subred
En IPv4, un número de 32 bits asociado con una dirección de IP para determinar en que porción de la red termina una dirección IP y en que porción del host empieza una dirección IP.

Máscara de subred de longitud variable
Ver VLSM.

Máscara wildcard
Cantidad de 32 bits que se usan de forma conjunta con una dirección IP para determinar cuáles son los bits de una dirección IP que deben omitirse al comparar esa dirección con otra dirección IP. La máscara wildcard se especifica al configurar las listas de acceso. Se la utiliza en IPv4.

Máscaras de subred de longitud variable (VLSM, Variable-Length Subnet Masks)
Máscara de subred de longitud variable.

Técnica usada para especificar una máscara de subred distinta para el mismo número de red principal a fin de identificar distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección IP disponible.

MCC
Conexión cruzada principal.

Armario para el cableado que sirve de punto central de una topología en estrella. La MCC es el punto donde se conecta el cableado backbone de LAN a Internet.

MCU
unidad de control multipunto

Dispositivo utilizado para admitir llamadas en conferencia con diversos participantes. Los participantes de la llamada en conferencia pueden enviar medios a la MCU, que los combina y envía a todos los participantes.

MD5
Message Digest 5.

Método de autenticación que requiere que cada router cuente con una clave y una identificación de clave únicas. El router utiliza un algoritmo que procesa la clave, el paquete de OSPF y el ID de la clave para generar un número encriptado. Cada paquete OSPF incluye el número encriptado. La clave nunca se transmite.

MDF
Instalación de distribución principal.

Recinto de comunicación primaria de un edificio. La MDF es el punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, los hubs y los routers. Se utiliza para conectar las líneas públicas o privadas que ingresan al edificio con las redes internas.

Memoria de contenido direccionable
Ver CAM.

Memoria flash
Memoria utilizada para almacenar y ejecutar el software IOS de Cisco. Cuando un router está desactivado, no se pierde el contenido de la memoria flash. Según el modelo de router, la memoria flash puede implementarse en chips de la memoria borrable programable de sólo lectura (EPROM) o en tarjetas de memoria compact flash externa . (Se la llama memoria flash porque el proceso de actualización del chip de las EPROM se denomina “flashing”.)

Mensaje de actividad
Broadcast enviado por un dispositivo de red para informar a otro dispositivo de red que el circuito virtual entre ambos sigue estando activo.

Mensaje de comprobación
Respuesta enviada por un router para establecer la identidad del emisor.

Mensaje de respuesta
Respuesta al mensaje que cada interfaz configurada para RIP envía pidiendo que todos los vecinos RIP envíen sus tablas de enrutamiento.

Mensaje de solicitud
Mensaje que cada interfaz configurada para RIP envía cuando se inicia un router pidiendo que todos los vecinos RIP envíen sus tablas de enrutamiento.

Método de corte adaptable
Tipo de conmutación en la que el flujo vuelve al modo de envío rápido cuando la cantidad de errores cae por debajo del umbral hasta un nivel aceptable.

Métrica
Información que utiliza un algoritmo de enrutamiento para determinar la mejor ruta de la red. Las métricas se almacenan en una tabla de enrutamiento. Las métricas incluyen ancho de banda, costo de comunicación, retardo, conteo de saltos, carga, MTU, costo de la ruta y confiabilidad.

Métrica compuesta
Método utilizado en una red EIGRP para calcular la mejor ruta para proporcionar un enrutamiento sin bucles y una convergencia rápida.

Métrica de enrutamiento
Estándar de medición que usa un algoritmo de enrutamiento que determina si una ruta es mejor que otra. Las métricas de enrutamiento se almacenan en tablas de enrutamiento y pueden incluir el ancho de banda, el costo de comunicación, el conteo de saltos, la carga, la unidad de transmisión máxima, el costo de la ruta y la fiabilidad.

Metro Ethernet
Sistema de red basado en tecnología de Ethernet que abarca un área metropolitana.

MIB
Base de información de administración.

Base de datos de información de administración de la red, utilizada y mantenida por un protocolo de administración de red como SNMP o el protocolo de información de administración común, también denominado CMIP. El valor de un objeto MIB se puede cambiar o recuperar usando comandos SNMP o CMIP. Los objetos MIB se organizan en una estructura de árbol que incluye ramificaciones públicas, o estándar, y privadas, o patentadas.

Microprocesador
Chip que contiene la unidad de procesamiento central del dispositivo.

Microsegmentación
División de una red en segmentos más pequeños, generalmente con la intención de aumentar el ancho de banda agregado en los dispositivos de red.

Microsegmento
División de una red en segmentos más pequeños, generalmente con la intención de aumentar el ancho de banda agregado en los dispositivos de red.

Microsoft Visio
Software de aplicación para diagramación publicado por Microsoft.

Migración en caso de fallos
Instancia en la que un dispositivo de red redundante se ocupa de la carga o función de otro dispositivo de forma automática si falla el dispositivo inicial. El esquema de migración en caso de fallos crea un sistema de respaldo para hardware y software críticos. El objetivo es reducir el impacto de las fallas del sistema al mínimo, al monitorear e identificar activamente las fallas del sistema.

Misión crítica
Tipo de red o proceso informático fundamental para la organización. El hecho de que se interrumpan con frecuencia o por demasiado tiempo las aplicaciones críticas pueden tener consecuencias negativas.

Modelo de diseño jerárquico
Representación de una red con una capa de acceso, una capa de distribución y una capa núcleo.

Modelo de red empresarial compuesta
Ver ECNM.

Módem
Dispositivo que convierte señales informáticas digitales en un formato que se puede enviar y recibir a través de líneas telefónicas analógicas. Módem es el término común para modulador-demodulador.

Modo automático
Designación de un puerto de un dispositivo como puerto de enlace troncal si el otro extremo se establece como enlace troncal o deseable.

Modo de transferencia asíncrona
Ver ATM.

Modo deseable
Designación de un puerto en un dispositivo como puerto de enlace troncal si el otro extremo se establece como enlace troncal o deseable.

Modo setup
Menú interactivo que permite crear un archivo de configuración inicial para un nuevo dispositivo de red o para un dispositivo en el cual se borró el archivo startup-config de NVRAM. Este modo puede ser usado también para modificar una configuración existente.

Modulación
Proceso mediante el cual se transforman las características de una señal eléctrica para representar información. Entre los tipos de modulación se cuentan la modulación de amplitud, la de frecuencia y la de amplitud de pulso.

Modular
Proceso mediante el cual se transforman las características de una señal eléctrica para representar información. Entre los tipos de modulación se cuentan la modulación de amplitud, la de frecuencia y la de amplitud de pulso.

Modularidad de red
La modularidad de red hace referencia a la organización de una red a partir subsistemas o módulos de menor tamaño que pueden diseñarse e implementarse de forma independiente. Los módulos pueden representar áreas que tengan diferente conectividad física o lógica. También designan las diferentes funciones que se producen en la red. La modularidad proporciona flexibilidad en el diseño de la red, y facilita la implementación y la resolución de problemas. A medida que se incrementa la complejidad de la red, los diseñadores pueden agregar nuevos módulos funcionales.

Módulo dependiente de protocolo
Ver PDM.

MOSPF
Multicast Open Shortest Path First.

Protocolo de enrutamiento multicast intradominio que se utiliza en las redes Open Shortest Path First. Se aplica una extensión al protocolo unicast OSPF base para admitir el enrutamiento multicast IP. La información de multicast se incluye en las publicaciones de estado de enlace de OSPF. El MOSPF genera un árbol de distribución para cada grupo y calcula un árbol para las fuentes activas enviadas a cada uno. El estado del árbol se guarda en la memoria caché y debe recalcularse cuando se produce un cambio en el estado de enlace, o cuando se supera el tiempo establecido para el caché.

También se conoce el MOSPF como OSPF multicast.

MPLS
Enrutamiento multiprotocolo de etiquetas.

Estándar utilizado para incrementar la velocidad del flujo de tráfico de una red. El proceso de MPLS marca cada paquete con la secuencia de la ruta a destino, en lugar de utilizar una tabla de enrutamiento. La conmutación de paquetes se lleva a cabo en la Capa 2 del modelo de referencia OSI. El MPLS es compatible con protocolos como IP, ATM y Frame Relay.

MS Visio
Software de aplicación para diagramación publicado por Microsoft.

MTU
Unidad máxima de transmisión.

Tamaño máximo de paquete, en bytes, que puede administrar una interfaz en particular.

Multiacceso
Tipo de red que permite que múltiples dispositivos se conecten y comuniquen de forma simultánea.

Multiacceso con broadcast
Tipo de enlace Ethernet identificado por OSPF, que es un estándar para una red de accesos múltiples que envía tráfico de broadcast.

Multiacceso sin broadcast
Ver NBMA.

Multicast
Paquetes individuales que la red copia y envía a un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de dirección de destino.

Multicast de protocolo de Internet
Ver multicast de IP.

Multicast independiente del protocolo
Ver PIM.

Multicast independiente del protocolo en modo denso
Ver PIM de modo denso.

Multicast independiente del protocolo en modo disperso
Ver PIM de modo disperso.

Multicast Open Shortest Path First
Ver MOSPF.

Multiplexación
Esquema que permite que múltiples señales lógicas se transmitan simultáneamente a través de un solo canal físico. Las señales se separan posteriormente en el extremo receptor.

Multiplexación estadística por división temporal
Ver STDM.

Multiplexación por división de longitud de onda densa
Ver DWDM.

Multiplexación por división temporal
Ver TDM.

NAC
Control de admisión a la red.

Método para evitar que un virus infecte un equipo controlando el acceso a una red. El NAC utiliza protocolos y productos de software para evaluar un host que intente iniciar sesión en una red. NAC determina la condición del host, denominada postura. Un host infectado puede ponerse en cuarentena. Un host con protección contra virus obsoleta recibe instrucciones para obtener una actualización. Un host sin infecciones y con protección contra virus obtiene acceso a la red.

El control de admisión a la red también se denomina control de acceso a la red.

NACL
Lista de servidores de acceso nombrada.

Estándar o formato extendido al que se hace referencia mediante un nombre descriptivo, en lugar de un número. Al configurar una NACL, el IOS del router utiliza un modo de subcomando de NACL.

NACL también se denomina ACL nombrada.

NAS
Almacenamiento con conexión a red.

Almacenamiento de datos de alta velocidad y gran capacidad, que agrupa grandes cantidades de unidades de disco que están directamente conectadas a la red y pueden ser utilizadas por cualquier servidor. Generalmente, un dispositivo de NAS se conecta a una red Ethernet y se le asigna su propia dirección IP.

NAT
Traducción de direcciones de red.

Estándar utilizado para reducir la cantidad de direcciones IP necesarias para que todos los nodos existentes dentro de la organización se conecten a Internet. La NAT permite que un grupo extenso de usuarios privados tengan acceso a Internet mediante la conversión de encabezados de paquete de un grupo reducido de direcciones IP públicas, y el seguimiento de éstas en una tabla.

NAT dinámica
Traducción de dirección de red dinámica.

Proceso de traducción de dirección de red que convierte una dirección IP local en una dirección IP global al asignar la primera dirección IP disponible de un grupo de direcciones públicas a un host interno. El host utiliza la dirección IP global asignada mientras dure la sesión. Cuando finaliza la sesión, la dirección global vuelve al grupo para ser usada por otro host.

NAT estática
Traducción de dirección de red estática.

Método por el cual un host interno con una dirección IP privada fija se marca siempre en el mapa con una dirección IP pública fija.

NAT-PT
Mecanismo ubicado entre una red IPv6 y una red IPv4 para traducir paquetes IPv6 a paquetes IPv4 y viceversa.

Navegador de funciones
Herramienta basada en la Web que se puede encontrar en el sitio Web de Cisco y ayuda a determinar qué funciones son compatibles con una imagen de software específica de IOS. Esta herramienta también puede utilizarse para encontrar qué imágenes de software de IOS son compatibles con determinadas funciones.

NBAR
Reconocimiento de aplicaciones basadas en red.

Utilidad de Cisco que lleva a cabo auditorías y análisis de tráfico. NBAR es una herramienta de descubrimiento de protocolos y clasificación que identifica el tráfico hasta la capa de aplicación. Proporciona estadísticas bidireccionales de interfaz y protocolo para cada flujo de tráfico que atraviese una interfaz. NBAR lleva a cabo la clasificación de subpuertos, que incluye la evaluación y la identificación más allá de los puertos de la aplicación. NBAR también reconoce protocolos basados en la Web y otros que utilizan asignaciones de puerto dinámicas de TCP y UDP.

NBMA
Acceso múltiple sin broadcast.

Redes que no son compatibles con broadcasting, como X.25, o en las cuales no es posible, como SMDS.

NCP
Protocolo de control de red.

Estándar que enruta y controla el flujo de datos entre un controlador de comunicaciones, en el que reside, y otros recursos de red.

NetFlow
Herramienta de contabilidad utilizada para analizar y proporcionar detalles sobre los patrones de tráfico de una red. NetFlow puede utilizarse para capturar la clasificación de tráfico o la prioridad asociada con cada flujo.

Networking de almacenamiento
Infraestructura que usa SAN y medidas de seguridad para satisfacer las necesidades de almacenamiento basado en red.

Networking de contenidos
Infraestructura que entrega contenido estático, fluido y dinámico a un usuario final, de forma confiable, escalable y segura. El networking de contenidos ofrece administración eficiente del ancho de banda y distribución de contenidos para contenido complejo de alto ancho de banda y la flexibilidad para adaptarse a nuevos contenidos y servicios.

El networking de contenidos también se denomina networking de entrega de contenidos o networking de contenidos de Internet.

NMP
Garantiza la continuidad comercial al mantener la red funcionando de manera eficiente. El mantenimiento de la red se debe programar durante períodos específicos, normalmente durante las noches y los fines de semana, a fin de minimizar el impacto sobre las operaciones comerciales.

NMS
Sistema de administración de red.

Sistema o aplicación que se utiliza para monitorear y controlar los dispositivos de red administrados, como CiscoWorks.

No contigua
Dirección de una red separada de las demás por una red o subred.

NOC
Centro de operaciones de red.

Organización que tiene la responsabilidad de mantener una red.

Normas de denominación IOS de Cisco
Sistema de denominación de archivos del sistema operativo en Internet.

Nombre de la imagen del software IOS de Cisco que representa el hardware, el conjunto de funciones, el formato, la versión de mantenimiento, la versión individual y la versión T, en ese orden.

Notas de la versión
Documentación que acompaña al software cuando se lo distribuye. Las notas de la versión incluyen la información más reciente, como la guía de usuario.

Notificación explícita de congestión hacia adelante
Ver FECN.

Notificación explícita de congestión hacia atrás
Ver BECN.

Número de host
Parte de una dirección IP que designa qué nodo de la subred se está direccionando.

El número de host también se conoce como dirección de host.

Número de la VLAN
Número asignado a una VLAN en el momento de su creación. El número de la VLAN puede ser cualquier número del rango disponible en el switch, con la excepción de VLAN1. Se considera que la asignación de nombres a las VLAN es una de las mejores prácticas de administración de red.

Número de revisión de configuración de VTP
Número de revisión de configuración del protocolo de enlace troncal de VLAN.

Orden numérico de mensajes multicast en una red. El número de revisión de configuración de VTP comienza en cero. Cuando se producen cambios en la red, el número de revisión de configuración aumenta en uno. Continúa aumentando hasta que alcanza 2.147.483.648. Si un mensaje tiene un número de revisión de configuración de VTP posterior al que tiene almacenado en la base de datos, el switch actualiza su base de datos de VLAN con esta nueva información.

NVRAM
Memoria de acceso directo no volátil. Se utiliza la NVRAM como ubicación de almacenamiento para el archivo de configuración de inicio de un router Cisco. Después de que el router carga su imagen IOS, se aplican los parámetros que se encuentran en la configuración de inicio.

OC
Portadora óptica.

Conjunto de protocolos físicos, como OC-1, OC-2, OC-3, definidos para las transmisiones de señales ópticas a través de la red óptica síncrona.

Los niveles de señal de OC agregan tramas de señal de transporte síncrono a la línea de fibra óptica a diferentes velocidades. La velocidad básica de un nivel de señal de OC es de 51.84 Mbps para OC-1. A partir de este punto, cada nivel de señal opera a una velocidad multiplicada por ese número. Por ejemplo, OC-3 se ejecuta a 155.52 Mbps (51,84 x 3 = 155.52).

Oficina central
Ver CO.

Onda portadora
Señal por la que se modulan y demodulan datos en una conexión analógica.

Open Shortest Path First (OSPF)
Open Shortest Path First.

Algoritmo de enrutamiento correspondiente a un protocolo de gateway interior jerárquico de estado de enlace, que reemplaza al protocolo de información de enrutamiento. Las características de OSPF incluyen enrutamiento por menor costo, enrutamiento de múltiples rutas y balanceo de carga.

Operación booleana AND
Elimina un patrón de bits; si se establece el comando con cero, se los sustituye por cero, mientras que si se lo establece con uno lo deja intacto, es decir, con “1”.

Orientado a los bits
En networking, se transmiten los datos mediante bits individuales, en lugar del byte completo.

OUI
Tres octetos asignados al administrador de hardware por IEEE en un bloque de direcciones LAN de 48 bits.

Panel de conexión
Conjunto de ubicaciones de pin y puertos que se puede montar en un bastidor o una consola de pared en el armario para el cableado. Un panel de conexión funciona como conmutador que conecta los cables de la estación de trabajo entre sí y al exterior.

PAP
Protocolo de autenticación de contraseña.

Estándar utilizado por pares PPP para autenticarse mutuamente en una red. Un router remoto envía una solicitud de autenticación al intentar conectarse a un router local. PAP pasa la contraseña y el nombre de host o de usuario. PAP no impide accesos no autorizados, pero identifica al usuario remoto. Luego, el router o servidor de acceso determina si se permite el acceso al usuario.

Paquete a través de SONET/SDH
Ver POS.

Paquete de actualización
Mensaje sobre la topología de la red enviado a un vecino. El paquete de actualización se agrega a la tabla de topología. Para enviar toda la información de topología completa a un nuevo vecino se requieren varias actualizaciones.

Paquete de consulta
Mensaje que se usa para consultar el valor de alguna variable o conjunto de variables.

Paquete de repetición
Información enviada cuando se recibe un paquete de consulta. Un paquete de repetición ayuda a DUAL a ubicar una ruta de sucesor en la red de destino. Las consultas pueden ser multicast o unicast. Las respuestas se envían siempre en unicast.

Paquete de saludo
Paquete multicast que se utiliza para detectar los dispositivos de una red y verificar las conexiones. El router utiliza el paquete de saludo para determinar la mejor conexión disponible.

Parámetro de negociación
Parámetro de un switch que detecta automáticamente el tipo de encapsulación del switch vecino.

Parte interesada
Persona u organización que tiene un interés en el éxito de un proceso.

PAT
Traducción de la dirección del puerto.

Estándar utilizado para reducir la cantidad de direcciones IP privadas internas a sólo una o varias direcciones IP públicas externas. La PAT permite que una organización conserve las direcciones en el conjunto de direcciones globales pues permite la traducción de puertos de origen en conexiones TCP o en conversaciones UDP. A continuación, se asignan distintas direcciones locales a la misma dirección global. La PAT proporciona la información única. La PAT es un subconjunto de la funcionalidad NAT.

Patentado
Dispositivo o software que no puede utilizarse con dispositivos o software de otros proveedores.

PBX
Central telefónica privada.

Conmutador telefónico digital o analógico ubicado en las instalaciones del suscriptor y que se usa para interconectar redes telefónicas privadas y públicas.

PDM
Módulo dependiente de protocolo.

Utilizado por EIGRP para tomar decisiones sobre tareas de enrutamiento específicas. Cada PDM mantiene tres tablas.

Perforación
Herramienta, accionada por un resorte, que se usa para cortar y conectar cables en un jack o en un panel de conexión.

Permitir
Dar consentimiento para que se lleve a cabo un proceso.

Período de espera

Colocación de un router en un estado en el que no publica ni acepta rutas por un período específico de tiempo, que se conoce como período de espera. La espera se usa para eliminar la información defectuosa acerca de una ruta de todos los routers de la red. Suele colocarse en espera una ruta cuando falla un enlace de esa ruta.

Período de inactividad

Porcentaje de tiempo en el que una red no está disponible debido a inactividad administrativa o a fallas en los equipos.

PIM

Multicast independiente del protocolo.

Estándar para la arquitectura de enrutamiento que permite agregar enrutamiento multicast de IP a una red IP existente. El PIM es independiente del protocolo de enrutamiento unicast. Puede funcionar en modo denso y modo disperso.

PIM de modo denso

Multicast independiente del protocolo en modo denso.

Cuando un receptor afectado por los estándares de PIM procesa grandes cantidades de tráfico. Los paquetes se envían por todas las interfaces de salida hasta que se produce la depuración y algunas salidas se truncan. Se supone que las redes descendentes reciben y utilizan los datagramas que se les envían. El PIM de modo denso se activa a través de datos y es similar a los protocolos de enrutamiento multicast típicos.

PIM de modo disperso

Multicast independiente del protocolo en modo disperso.

Cuando los receptores afectados por los estándares de PIM están ampliamente distribuidos, el PIM de modo disperso trata de restringir la distribución de datos de modo que una cantidad mínima de routers de la red los reciban. Los paquetes se envían sólo si se los solicita explícitamente en el punto de rendezvous. Se supone que las redes descendentes no necesariamente utilizan los datagramas que se les envían.

Placa frontal

Componente de protección que, por lo general, se instala en la parte frontal de un dispositivo.

Plan de continuidad de la empresa

Pasos que deben seguirse a fin de continuar las operaciones comerciales en caso de que ocurra un desastre natural o provocado por el hombre.

Plan de mantenimiento de red

Ver NMP.

Plan de seguridad de la empresa

Medidas de control físicas, organizativas y del sistema que deben tomarse a fin de proteger la red y los bienes de información.

Plan de supervisión de la red

Información utilizada por un administrador de red para evaluar el estado de una red.

Plano de control

Conjunto de procesos que se ejecutan en el nivel de proceso en el procesador de ruta. Los procesos del plano de control proporcionan colectivamente un control de alto nivel para la mayoría de las funciones de IOS de Cisco.

PoE
Power over Ethernet.

Estándar de alimentación para dispositivos de red por cable Ethernet. IEEE 802.3af y Cisco especifican dos métodos de PoE distintos. Los equipos de alimentación de energía y los dispositivos eléctricos de Cisco son compatibles con ambos métodos de PoE.

Política de seguridad
Descripción de las medidas de protección del sistema, físicas y de funcionamiento implementadas en una organización.

Políticas de calidad de servicio
Procedimientos definidos y utilizados en los procesos de calidad de servicio.

POP
Punto de presencia.

Conexión física entre una instalación de comunicación proporcionada por un ISP o empresa telefónica local, y la instalación de distribución principal de una organización.

Portadora
Onda electromagnética o corriente alterna de una sola frecuencia, adecuada para modulación por parte de otra señal portadora de datos.

Portadora óptica
Ver OC.

Portadora T
Cualquiera de los sistemas portadores de telecomunicaciones multiplexados digitalmente.

PortFast
Mejora de STP que hace que los puertos de acceso pasen de inmediato al estado de envío, y evita los estados de escucha y aprendizaje. El uso de PortFast en los puertos de acceso que están conectados a una sola estación de trabajo o servidor permite que estos dispositivos se conecten a la red de inmediato.

POS
Paquete a través de SONET/SDH.

Tipo de estructura de red compatible con SONET y SDH, que transmite grandes cantidades de voz y datos a través de grandes distancias mediante cable de fibra óptica.

POST
Autocomprobación de encendido.

Proceso utilizado para evaluar el hardware del dispositivo después de encenderlo.

POTS
Servicio telefónico analógico convencional. Ver PSTN.

Power over Ethernet
Ver PoE.

PPDIOO
Proceso de seis fases de Cisco Lifecycle Services para admitir redes en evolución. En cada fase, se definen las actividades necesarias para implementar y hacer funcionar correctamente las tecnologías de Cisco. PPDIOO detalla cómo optimizar el rendimiento a través del ciclo de vida de una red.

PPP
Protocolo punto a punto.

Estándar que proporciona conexiones de router a router y de host a red a través de circuitos síncronos y asíncronos.

PPTP
Protocolo de tunneling punto a punto.

El protocolo de tunneling punto a punto (PPTP, Point-to-Point Tunneling Protocol) fue desarrollado por Microsoft. Se describe en RFC2637. Se utiliza mucho el PPTP en software cliente de Windows para crear VPN en redes TCP/IP.

PQ
Cola según prioridad.

Función del enrutamiento en la que se toman en cuenta las características de una trama, como el tamaño de los paquetes y el tipo de interfaz, a fin de determinar el orden en que se envía.

Prefijo de dirección
Patrón que coincide con los bits de una dirección IP. Por ejemplo, 130.120.0.0/16 coincide con los primeros 16 bits de la dirección IP 130.120.0.0, es decir, 130.120. En otro ejemplo, 12.0.0.0/12 coincide con 12.0.2.3, 12.2.255.240 y 12.15.255.255, pero no coincide con 12.16.0.1.

Prefijo de enrutamiento
Patrón para hacer coincidir rutas en una tabla de enrutamiento.

preparar, planear, diseñar, implementar, funcionar y elegir
Ver PPDIOO.

Primera milla
Sección de medio físico que sale de la ubicación del cliente en dirección a la oficina central de un proveedor de servicios.

Privacidad equivalente por cable
Ver WEP.

Proceso de arranque
Actividad de inicio de un dispositivo informático. El proceso de arranque tiene tres pasos. En primer lugar, se prueban los componentes internos. Luego, se ubica e inicia el sistema operativo. Por último, se carga la configuración inicial. Después de completar el proceso de arranque, el dispositivo se encuentra en funcionamiento.

Productos anteriores
Estilos más antiguos de hardware o software que todavía están en uso.

Programas detectores de paquetes
Herramienta que analiza los flujos de tráfico en función del origen y el destino del tráfico, además del tipo de tráfico que se está enviando. El análisis con programas detectores de paquetes puede utilizarse para tomar decisiones sobre cómo administrar el tráfico de manera más eficiente.

Protocolo de administración de grupos de Internet
Ver IGMP.

Protocolo de autenticación de contraseña
Ver PAP.

Protocolo de autenticación de intercambio de señales
Ver CHAP.

Protocolo de border gateway
Ver BGP.

Protocolo de configuración dinámica de host (Dynamic Host Configuration Protocol)
Ver DHCP.

Protocolo de control de enlace
Ver LCP.

Protocolo de control de intercambio de paquetes de internetwork
Ver IPXCP.

Protocolo de control de red
Ver NCP.

Protocolo de control de transporte en tiempo real
Ver RTCP.

Protocolo de control del protocolo de Internet.
Ver IPCP.

Protocolo de datagramas del usuario (UDP)
Ver UDP.

Protocolo de descubrimiento de Cisco
Ver CDP.

Protocolo de descubrimiento de gateway (Gateway Discovery Protocol)
Ver GDP.

Protocolo de enlace de dos vías
Proceso de autenticación usado en PAP. Durante el protocolo de enlaces de dos vías, un dispositivo busca el usuario y la contraseña del dispositivo que está haciendo la llamada para confirmar que la información concuerde con la almacenada en la base de datos.

Protocolo de enlace de tres vías
Serie de sincronizaciones y acuses de recibo usada por TCP para abrir una conexión.

Protocolo de enlace troncal virtual
Ver VTP.

Protocolo de enrutamiento
Estándar que usa un algoritmo de enrutamiento. Entre los ejemplos de protocolos de enrutamiento se incluyen: IGRP, OSPF y RIP.

Protocolo de enrutamiento de gateway interior mejorado
Ver EIGRP.

Protocolo de enrutamiento multicast de vector distancia
Ver DVMRP.

Protocolo de enrutamiento sin clase
Estándar que proporciona instrucciones a los datos para enviar una máscara de subred con todos los paquetes de actualización de enrutamiento. Es necesario un protocolo de este tipo cuando la máscara no puede presuponerse o determinarse por el valor del primer octeto. Los protocolos de enrutamiento sin clase incluyen RIPv2, EIGRP y OSPF.

Protocolo de envío de Capa 2
Ver Protocolo L2F.

Protocolo de gateway exterior
Ver EGP.

Protocolo de gateway interior
Ver IGP.

Protocolo de información de enrutamiento
Ver RIP.

Protocolo de información de enrutamiento de próxima generación
Ver RIPng.

Protocolo de información de enrutamiento versión 2
Ver RPIv2.

Protocolo de Internet móvil
Ver IP móvil.

Protocolo de Internet versión 4
Ver IPv4.

Protocolo de Internet versión 6
Ver IPv6.

Protocolo de mensajes de control de Internet (Internet Control Message Protocol)
Ver ICMP.

Protocolo de punto de acceso liviano
Ver LWAPP.

Protocolo de Rapid Spanning Tree (RSTP, Rapid Spanning Tree Protocol)
Protocolo Rapid Spanning-Tree.

Actualización a los estándares del Protocolo Spanning-Tree que reduce el tiempo necesario para que se establezcan las conexiones a los puertos del switch.

Protocolo de resolución de direcciones de línea serial
Ver SLARP.

Protocolo de resolución de direcciones inverso
Ver ARP inverso.

Protocolo de saludo
Estándar que utilizan los sistemas OSPF para establecer y mantener relaciones con los vecinos. El protocolo de saludo es un protocolo interno que utiliza una métrica de enrutamiento basada en la cantidad de tiempo que demora un paquete en viajar desde el origen hasta el destino.

Protocolo de shell remoto
Ver rsh.

Protocolo de transferencia de archivos (File Transfer Protocol)
Ver FTP.

Protocolo de transferencia de archivos trivial (Trivial File Transfer Protocol)
Ver TFTP.

Protocolo de transferencia de hipertexto (Hypertext Transfer Protocol)
Ver HTTP.

Protocolo de transporte confiable (RTP)
Ver Protocolo de transporte en tiempo real.

Protocolo de transporte en tiempo real
Ver RTP.

Protocolo de tunneling de Capa 2
Ver L2TP.

Protocolo de tunneling punto a punto
Ver PPTP.

Protocolo de vector distancia
Tipo de estándares que usan la distancia para seleccionar el mejor camino. Entre los ejemplos de un protocolo de vector distancia se incluyen RIP, IGRP y EIGRP.

Protocolo L2F
Protocolo de envío de Capa 2.

El Protocolo de envío de Capa 2 (L2F) es un protocolo desarrollado por Cisco que admite la creación de redes privadas de marcado telefónico virtual seguro mediante Internet a través del tunneling de tramas de Capa 2.

Protocolo punto a punto (Point-to-Point Protocol)
Ver PPP.

Protocolo Rapid Spanning Tree
Ver RSTP.

Protocolo Rapid Spanning-Tree mejorado
Ver RSTP+.

Protocolo simple de transferencia de correo (Simple Mail Transfer Protocol)
Ver SMTP.

Protocolo Spanning Tree
Ver STP.

Protocolos de Link-State
Tipo de estándares, como OSPF y IS-IS, utilizados en un diseño de red jerárquico. Los protocolos de Link-State ayudan a administrar los procesos de conmutación de paquetes en grandes redes.

Proveedor de servicios
Ver SP.

Proveedor de servicios de telecomunicaciones
Ver TSP.

Proyecto terminado
Diagrama que muestra el diseño original y cualquier cambio que se haya aplicado a la topología de la red.

Prueba de aceptación de nivel de sistema
Práctica de verificar si una red cumple los objetivos comerciales y los requerimientos de diseño. Los resultados de la prueba de aceptación de nivel de sistema se registran y forman parte de la documentación que se entrega al cliente.

Prueba de concepto
Prueba de que un diseño funciona según lo esperado.

Prueba y error
Técnica de resolución de problemas que aprovecha la experiencia y las pruebas para solucionar un problema.

PSN
Red conmutada por paquetes.

Red que usa la tecnología de conmutación por paquetes para la transferencia de datos.

PSTN
Red pública de telefonía conmutada.

Término general que se refiere a las diversas redes y servicios telefónicos que existen a nivel mundial.

PSTN también se conoce como servicio telefónico analógico convencional o POTS.

Publicación
Proceso del router en el que las actualizaciones de enrutamiento o servicio que contienen listas de rutas utilizables se envían a intervalos especificados a los routers de la red.

Publicación de estado de enlace
Ver LSA.

Publicación de resumen
Nombre de dominio y número de revisión de configuración actual de VTP que un switch Catalyst emite periódicamente.

Publicaciones de subconjunto
Mensaje VTP que contiene nueva información de la VLAN según la publicación de resumen.

Puente
Dispositivo que conecta y transfiere paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Un puente opera en la capa de enlace de datos del modelo de referencia de OSI. En general, filtra, reenvía o inunda una trama entrante basándose en la dirección MAC de esa trama.

Puente raíz
Dispositivo designado para el envío de paquetes en una implementación de spanning-tree que recibe información de topología y notifica a otros puentes de la red cuando se requieren cambios en la topología. El puente raíz evita los bucles y suministra un medio de defensa contra las fallas de enlace.

El puente raíz también se denomina switch raíz.

Puenteo Frame Relay
Técnica que se describe en la RFC 1490, que usa el mismo algoritmo spanning-tree que otras funciones de puenteo, pero permite que los paquetes se encapsulen para su transmisión a través de la red Frame Relay.

Puerto
1) Interfaz de un dispositivo de red, como un router o un switch. 2) Proceso de capa superior que recibe información de capas inferiores. 3) Conector hembra de un panel de conexión.

Puerto de acceso
Ruta a un dispositivo que no crea bucles en una red conmutada y siempre pasa al estado de reenvío si hay un host conectado.

Puerto de enlace troncal
Enlace punto a punto que conecta un switch a otro switch, un router o un servidor. El enlace troncal transporta tráfico por múltiples VLAN por el mismo enlace. Las VLAN son multiplexadas por el enlace con un protocolo de enlace troncal.

Puerto designado
Interfaz de un dispositivo que envía tráfico hacia el puente raíz pero no se conecta con la ruta de menor costo.

Puerto raíz
Puerto designado STP que proporciona la ruta menos costosa de vuelta al puente raíz.

Puerto uplink
Puerto de alta velocidad que se conecta a las áreas que presentan mayor demanda de ancho de banda, como otro switch, un servidor central u otras redes.

Puertos bloqueados
1) En un sistema de conmutación, una condición en la que no hay ninguna ruta disponible para completar un circuito. 2) Condición en la que una actividad no puede comenzar hasta que se lleve a cabo otra.

Puertos de acceso
Ruta a un dispositivo que no crea bucles en una red conmutada y siempre pasa al estado de reenvío si hay un host conectado.

Puertos de enlace troncal
Enlace punto a punto que conecta un switch a otro switch, un router o un servidor. El enlace troncal transporta tráfico por múltiples VLAN por el mismo enlace. Las VLAN son multiplexadas por el enlace con un protocolo de enlace troncal.

Punto a punto T1
Conectividad WAN que ofrece control sobre la calidad de servicio disponible.

Punto de acceso
Ver AP.

Punto de acceso inalámbrico
Sitios físicos conectados en una red que transmite señales para dispositivos inalámbricos.

Punto de acceso liviano
Ver LWAP.

Punto de código de servicios diferenciados
Ver DSCP.

Punto de presencia
Punto de presencia.

Conexión física entre una instalación de comunicación proporcionada por un ISP o empresa telefónica local, y la instalación de distribución principal de una organización.

PVC
Circuito virtual permanente.

Conexión que ahorra ancho de banda porque el circuito ya está establecido con anticipación.

PVP
Ruta virtual permanente.

Pasaje que consta de circuitos virtuales permanentes.

PVRST+
Según VLAN Rapid Spanning Tree +.

Implementación de Cisco de una instancia de RSTP por VLAN.

Q.922A
Especificación de la UIT-T para la encapsulación Frame Relay.

QoS
Calidad de servicio.

Estándar para la supervisión y el mantenimiento del rendimiento de nivel de transmisión y servicio, como ancho de banda disponible para transmisión de datos y frecuencia de errores.

Radiofrecuencia
Ver RF.

Ráfaga excesiva
Ver Be.

Ráfaga garantizada
Mayor transferencia de datos por encima de la velocidad garantizada que se acepta temporalmente en un circuito virtual permanente. Una ráfaga garantizada no se etiqueta para descarte en caso de congestión en la red. Una ráfaga garantizada se especifica en bytes o celdas.

Ráfaga suscrita
Ver Bc.

RAM
Memoria de acceso aleatorio.

RD
Distancia notificada.

Distancia hacia un destino tal como la publica un vecino.

Reconocimiento de aplicaciones basadas en red
Ver NBAR.

Red conmutada por paquetes
Ver PSN.

Red de área extensa
Ver WAN.

Red de área local
Ver LAN.

Red de área local inalámbrica dedicada
Ver LAN dedicada.

Red de área local virtual
Ver VLAN.

Red de área virtual local de administración
Ver VLAN de administración.

Red de conexión única
Red que tiene una sola conexión con un router.

Red determinista
Sistema diseñado para la transmisión de datos a fin de seguir una ruta predefinida durante un plazo exacto.

Red empresarial
Red que integra todos los sistemas dentro de una empresa u organización. Una red empresarial se diferencia de una WAN en el sentido de que pertenece y se mantiene en forma privada.

Red global externa
Red conectada a un router, que es externa a LAN y que no reconoce las direcciones privadas que se asignan a los host en la LAN interna.

Red heterogénea
Sistema de dispositivos distintos que ejecutan protocolos distintos y pueden ser compatibles con diversas funciones o aplicaciones que pueden trabajar juntas.

Red híbrida
Internetwork compuesta por más de un tipo de tecnología de red, como LAN y WAN.

Red IP
Una red que utiliza el protocolo IP, que forma parte TCP/IP.

Red jerárquica
Técnica de diseño que divide la red en capas para evitar la congestión y reducir el tamaño de los dominios de fallas. El modelo de diseño jerárquico de Cisco utiliza capas de acceso, distribución y núcleo.

Red local interna
Espacio de red de direccionamiento privado, conectado a la interfaz de un router. La red local interna se utiliza para superar la escasez de direcciones IP públicas.

Red no contigua
Sistema de redes con subredes no adyacentes o subredes que están separadas de las demás por otras redes.

Red plana
Sistema en el que todas las estaciones pueden alcanzarse sin tener que atravesar un dispositivo, como ser un router.

Red privada virtual
Ver VPN.

Red privada virtual de acceso remoto
Ver VPN de acceso remoto.

Red pública de telefonía conmutada
Ver PSTN.

Red óptica síncrona
Ver SONET.

Redes conmutadas por celdas
Esquema de comunicación de datos basado en estructuras de celdas de longitud fija. En una red conmutada por celdas, la celda de longitud fija alcanza una velocidad mayor de transmisión que las que utilizan paquetes de longitud variable. ATM es un ejemplo de tecnología de conmutación en una red que proporciona todo el ancho de banda del enlace cuando una estación se comunica con el switch.

Redes de área local virtuales (VLAN)
Red de área local virtual.

Grupo de dispositivos alojados en una red, generalmente estaciones de usuarios finales, que se comunican como si estuvieran conectados al mismo segmento de la red aún cuando pueden estar en segmentos distintos. Las VLAN se configuran en switches de grupo de trabajo. Los switches con VLAN pueden interconectarse usando protocolos VLAN de enlace troncal.

La VLAN también se denomina LAN virtual.

Redes privadas virtuales (VPN)
Ver VPN.

Redirector
Software que intercepta peticiones para recursos dentro de un equipo y luego las envía al host correspondiente para procesar la transacción de forma más eficiente. El redirector crea una llamada remota que se envía al software de protocolo de capa inferior que pueda cumplir la solicitud.

Redistribución
Proceso que consiste en incluir información de enrutamiento detectada a través de un protocolo de enrutamiento en los mensajes de actualización de otro protocolo de enrutamiento.

Redistribución de ruta
La ruta predeterminada es propagada desde el router de extremo hasta otros routers internos.

Redundancia
1) Duplicación de los componentes de una red, como dispositivos, servicios o conexiones, con el propósito de mantener la operabilidad si alguna herramienta falla. 2) Porción de la información total contenida en un mensaje que puede ser eliminada sin perder el contexto.

Reemplazo avanzado
Parte de un acuerdo SMARTnet que se ofrece como parte de una mejora del servicio al cliente.

Reenvío
Proceso que se usa para enviar una trama desde un puerto hacia su destino, a través de un dispositivo de internetworking. Entre los dispositivos que envían tramas se cuentan los hosts, los repetidores, los puentes y los routers.

Registro
Proceso de registro y acceso a los detalles sobre paquetes que se permitieron o rechazaron en una red.

Registro de configuración
En los routers Cisco, un valor de 16 bits que el usuario puede configurar y que determina cómo funciona el router durante el inicio. Es posible guardar el registro de configuración en el hardware o en el software. En el hardware, el valor para cada posición del bit se establece usando un jumper. En el software, los valores para las posiciones del bit se establecen especificando un valor hexadecimal mediante los comandos de configuración.

Reserva del ancho de banda
Proceso por el que se asigna ancho de banda a los usuarios y las aplicaciones a los que una red brinda servicio. La reserva del ancho de banda implica la asignación de prioridad a los distintos flujos de tráfico según características críticas y de sensibilidad a las demoras. Si se congestiona la red, el tráfico de menor prioridad se puede descartar.

La reserva del ancho de banda también se denomina asignación de ancho de banda.

Respaldo usando una línea telefónica
Característica de los routers Cisco que proporciona protección contra el tiempo de inactividad de la WAN al permitir que el administrador de red configure una línea serial de respaldo a través de una conexión conmutada por circuito.

Respuesta de voz interactiva
Ver IVR.

Retardo
1) La cantidad de tiempo que hay entre el inicio de una transacción por parte del emisor y la primera respuesta recibida por el emisor. 2) La cantidad de tiempo necesaria para mover un paquete desde el origen hacia el destino a través de una ruta específica.

Retardo de propagación
Cantidad de tiempo que se requiere para que los datos viajen a través de una red, desde el origen hasta el destino.

RF
Radiofrecuencia.

Ondas electromagnéticas generadas por CA y enviadas a una antena dentro del espectro electromagnético. Las redes de televisión por cable y de banda ancha usan la tecnología RF. Las WLAN usan RF para transmitir datos.

RFI
Interferencia de radiofrecuencia.

Ruido que interfiere con la información que se transmite a través de un cable de cobre no blindado.

RFP
Solicitud de propuesta.

Documentación formal que una organización presenta a potenciales proveedores pidiendo información sobre qué tipo de servicios o productos provee.

RFQ
Solicitud de cotización.

Documentación formal que una organización presenta a potenciales proveedores pidiendo una propuesta o cotización de costo de los servicios o productos ofrecidos. Se emite una RFQ una vez determinadas las especificaciones.

RIP
Protocolo de información de enrutamiento.

Estándar de enrutamiento de vector distancia que usa el conteo de saltos como matriz de enrutamiento.

RIPng
Protocolo de información de enrutamiento de próxima generación.

Estándar de enrutamiento de vector distancia con un límite de 15 saltos que usa envenenamiento en reversa y horizonte dividido para evitar routing loops. Es similar a RIPv2 y está basado en IPv4 RIPv2, pero usa IPv6 como transporte. La dirección del grupo multicast FF02::9 identifica todos los routers con RIPng activado.

RIPv2
Protocolo de información de enrutamiento versión 2.

Estándar de enrutamiento de vector distancia basado en RIPv1 con extensiones adicionales para adecuarse a los entornos de enrutamiento modernos. El RIPv2 es compatible con actualizaciones de VLSM, autenticación y multicast. El RIPv2 está definido en RFC 1723 y es compatible con versiones IOS 11.1 y posteriores.

Rivest, Shamir y Adleman
Ver RSA.

Rlogin
Inicio de sesión remoto.

Programa de emulación de terminal que se ofrece en la mayoría de las implementaciones UNIX para acceder a dispositivos remotos, como Telnet.

RMON
Supervisión remota.

Especificación de agente de base de información de administración que se describe en la RFC 1271 y define las funciones para la supervisión remota de los dispositivos conectados a la red. RMON provee capacidades de supervisión, detección de problemas y generación de informes.

Robo
Cuando un pirata informático obtiene acceso ilegal a un sistema mediante una conexión autenticada.

ROM
Memoria de sólo lectura (ROM). Por lo general, la ROM se utiliza como el área de memoria desde la cual un router Cisco comienza el proceso de inicio, es compatible con la autocomprobación de encendido y admite el entorno de diagnóstico del Monitor de ROM.

Router
Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra, sobre la base de la información de la capa de red.

Router activado por voz
Dispositivo que convierte señales telefónicas de voz análogas en paquetes IP. El router activado por voz envía paquetes IP entre distintas ubicaciones.

Router de borde de área
Ver ABR.

Router de borde del sistema autónomo
Ver ASBR.

Router designado
Router designado por el protocolo de saludo OSPF en una red OSPF que tiene al menos dos routers conectados. Un router designado genera las LSA. Permite una reducción en la cantidad de adyacencias requeridas, lo que reduce la cantidad de tráfico de protocolo de enrutamiento y el tamaño de la base de datos topológica.

Router designado de respaldo
Ver BDR.

Router núcleo
Router en una topología en estrella conmutada por paquetes que forma parte del backbone. El router núcleo funciona como la vía única por la que debe pasar todo el tráfico de las redes periféricas camino a otras redes periféricas.

Router-on-a-stick
Configuración en un router que determina que si el destino de la VLAN se encuentra en el mismo switch que la VLAN de origen, el router debe enviar el tráfico de vuelta al router de origen con los parámetros de la subinterfaz del ID de la VLAN de destino.

Routers vecinos
En OSPF, routers que tienen interfaces en una red común. En una red de acceso múltiple, los vecinos se detectan de forma dinámica a través del protocolo de saludo OSPF.

RPC
Llamada de procedimiento remoto.

Comunicación desde un programa local a un programa remoto para solicitar el uso temporal de los servicios disponibles en un programa remoto.

RSA
Rivest, Shamir, y Adleman.

Algoritmo para encriptación asimétrica de claves públicas. El RSA fue el primer algoritmo adecuado para firmar y encriptar. Fue uno de los primeros grandes avances en criptografía de claves públicas.

RSSI
Indicador de intensidad de la señal del receptor.

Medición de la intensidad de la señal RF recibida por una aplicación WLAN.

RSTP
Protocolo Rapid Spanning-Tree.

Actualización a los estándares del Protocolo Spanning-Tree que reduce el tiempo necesario para que se establezcan las conexiones a los puertos del switch.

RSTP+
Protocolo Rapid Spanning-Tree Mejorado.

Tipo de protocolo Spanning-Tree que incrementa la velocidad de convergencia.

RTCP
Protocolo de control de transporte en tiempo real.

Estándar de control para RTP que monitorea y proporciona sugerencias sobre la calidad del servicio de un enlace de transmisión.

RTP
Protocolo de transporte en tiempo real.

Estándar para la funcionalidad y el formato de paquetes que se usa comúnmente en redes IP para transmitir datos en tiempo real, como audio, video o datos de simulación, mediante servicios de red en multicast o en unicast. El RTP provee servicios, como identificación de tipo de contenido, numeración de secuencias, marca horaria y envío de supervisión a aplicaciones en tiempo real.

RU
Unidad de bastidor.

Estándar de medición de factor de forma para el espacio vertical que ocupa el equipo. Una unidad de bastidor tiene una altura de 4,4 cm. Un dispositivo se mide en RU. Si un dispositivo tiene 4,4 cm de alto, tiene 1RU. Si tiene 8,8 cm de alto, mide 2RU.

Runt
Trama que tiene menos de 64 bytes, generalmente, como resultado de una colisión. En la conmutación libre de fragmentos, el switch lee los primeros 64 bytes de la trama antes de comenzar a enviarla al puerto de destino. La comprobación de los primeros 64 bytes garantiza que el switch no envíe fragmentos debidos a colisiones.

Ruta
Ruta entre los dispositivos de origen y destino.

Ruta de menor costo
Cálculo de un switch para encontrar una ruta que utilice la menor cantidad posible de ancho de banda para cada enlace que deba alcanzar el puente raíz.

Ruta de sucesor
Ruta principal de mismo costo, sin bucles, con la menor métrica hasta el destino determinado por la topología y registrada en la tabla de enrutamiento.

Ruta estática
Ruta configurada y especificada en la tabla de enrutamiento de forma manual. Una ruta estática tiene prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico.

Ruta estática flotante
Ruta que se configura manualmente y se ingresa en la tabla de enrutamiento que tiene configurada una distancia administrativa mayor que la distancia administrativa de una ruta dinámica. Esta ruta sólo se utiliza si la ruta dinámica existente no se encuentra disponible.

Ruta predeterminada
Ruta de un paquete de red utilizada de forma predeterminada, o como último recurso, cuando los hosts de destino no figuran en la tabla de enrutamiento.

Ruta principal
Cuando la sumarización predeterminada no está habilitada, las actualizaciones incluyen información de subredes. La tabla de enrutamiento instala entradas para cada subred y una entrada para el resumen de rutas. La ruta principal es anunciada por el router de sumarización, siempre que, al menos, una ruta específica de su tabla de enrutamiento coincida con la ruta principal.

La ruta principal se denomina resumen de ruta y la ruta secundaria se denomina ruta de subred.

Ruta quad zero
Ruta en la que la dirección de red y la máscara de subred se especifican en 0.0.0.0. El comando utiliza la dirección del siguiente salto o los parámetros de la interfaz de salida.

Ruta secundaria
Ruta de subred en una red EIGRP.

Ruta virtual
Agrupación lógica de circuitos virtuales que conectan dos sitios.

Ruta virtual permanente
Ver PVP.

Sacudida
Problema en el enrutamiento en el que una ruta publicada entre dos dispositivos alterna entre dos rutas debido a fallas intermitentes en la red.

Saliente
Una de dos direcciones en las que viaja un paquete en una red a través de una interfaz. Un paquete saliente es el que sale de un dispositivo.

Salto
Transferencia de un paquete de datos entre dos dispositivos de red, por ejemplo, routers.

SAN
Storage area network, SAN.

Plataforma de comunicación de datos que interconecta servidores y almacenamiento en gigabaudios. Al combinar modelos de red LAN con el rendimiento del servidor y con la capacidad de almacenamiento masivo, la SAN elimina los problemas de ancho de banda y las limitaciones de escalabilidad creadas por arquitecturas anteriores basadas en el bus SCSI.

Saturar
Técnica utilizada por los switches para transmitir tráfico que se recibe en una interfaz a todas las demás interfaces del dispositivo, excepto a la interfaz en la que se recibió originalmente la información.

SDH
Jerarquía digital síncrona.

Estándar europeo que define un conjunto de estándares de velocidad y formato que se transmiten usando señales ópticas a través de la fibra óptica. El SDH es similar a SONET, con una velocidad SDH básica de 155,52 Mbps, designada en STM-1.

SDM
Administración de dispositivos de seguridad de Cisco.

Herramienta de administración de dispositivos basada en la Web para un router Cisco IOS basado en software. Simplifica la configuración de router y seguridad a través de un asistente inteligente que se utiliza para implementar, configurar y supervisar un router Cisco sin necesidad de tener conocimientos del CLI.

SDRAM
Memoria síncrona de acceso directo aleatorio. Una forma de DRAM.

Secreto compartido
Contraseña conocida entre dispositivos.

Secuencia de verificación de trama
Ver FCS.

Segmento
1. Sección de una red limitada por puentes, routers o switches.

2. Circuito eléctrico continuo en una LAN que usa topología de bus que, en general, se conecta a otros segmentos con repetidores.

3. Unidad de información única de la capa lógica de transporte.

Un segmento que es una unidad lógica de información puede denominarse también datagrama, trama, mensaje o paquete.

Segmento de tiempo
Periodo durante el cual una conversación dispone por completo de los medios físicos. El ancho de banda es asignado a cada canal o intervalo de tiempo. En TDM estándar, si un emisor no tiene nada para decir, el intervalo de tiempo no se utiliza, por lo que se desperdicia ancho de banda valioso. En STDM, se hace un seguimiento de las conversaciones que requieren ancho de banda extra. Luego, se reasignan dinámicamente los intervalos de tiempo que se encuentren en desuso, según sea necesario para minimizar el uso del ancho de banda.

Seguridad
Protección de datos y hardware contra daños y accesos no deseados.

Seguridad de IP
Ver IPSec.

Seguridad de protocolo de Internet
Ver IPSec.

Según VLAN Rapid Spanning Tree Plus
Ver PVRST.

Señal de temporización
Indicador de la velocidad a la que se desplazan los datos en el bucle local.

Señal de transporte síncrono de nivel 1
Ver STS-1.

Señal de transporte síncrono de nivel 3, concatenada
Ver STS-3c.

Señal digital de nivel 0
Ver DS0.

Señal digital de nivel 1
Ver DS1.

Señal digital de nivel 3
Ver DS3.

Servicio de correo electrónico
Ver correo electrónico.

Servicio de datos multimegabit conmutado
Ver SMDS.

Servicio de distribución intermedia (IDF, Intermediate Distribution Facility)
servicio de distribución intermedia.

Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella. El IDF tiene una trama con una conexión cruzada desde los medios de cable del usuario hasta los circuitos de línea de usuario y puede servir como punto de distribución de cables con múltiples pares desde la trama de distribución principal. El IDF depende del MDF.

Servidor
Programa de software o nodo que provee datos o servicios a pedido de los clientes.

Servidor de autenticación
Servidor que controla la frecuencia y la temporización de las comprobaciones a fin de evitar ataques a la red.

Servidor de política de administración de VLAN (VMPS)
Ver VMPS.

Shell Seguro
Ver SSH.

Siguiente salto
Interfaz en un router conectado que acerca los datos a su destino final.

Simple Network Management Protocol
Ver SNMP.

Sin etiquetar
Tráfico sin ID de la VLAN que debe atravesar el enlace configurado según 802.1q. Entre los ejemplos de tráfico sin etiquetar se cuentan el protocolo de descubrimiento de Cisco, VTP y ciertos tipos de tráfico de voz. El tráfico sin etiquetar minimiza los retrasos asociados con la inspección de la etiqueta de ID de la VLAN.

Sistema autónomo
Ver AS.

Sistema de administración de red
Ver NMS.

Sistema de alimentación ininterrumpida
Ver UPS.

Sistema de denominación de archivos del sistema operativo en Internet
Ver normas de denominación IOS de Cisco.

Sistema de denominación de dominios
Ver DNS.

Sistema de detección de intrusión
Ver IDS.

Sistema de información de colaboración distribuida
Programas de base de datos y aplicaciones compatibles con actividades de colaboración asíncrona en línea.

Sistema de nombres de dominios
Ver DNS.

Sistema de prevención de intrusión
Ver IPS.

Sistema intermedio a Sistema intermedio
Ver IS-IS.

Sistemas de detección de intrusión (IDS)
Ver IDS.

Sistemas de prevención de intrusión
Ver IPS.

SLA
Acuerdo de nivel de servicio.

Contrato vinculante entre un proveedor de servicios de red y el usuario final que requiere un cierto nivel de servicio.

SLARP
Protocolo de resolución de direcciones de línea serial.

Estándar que asigna una dirección al extremo de un enlace serial si el otro extremo ya fue configurado. El SLARP supone que cada línea serial es una subred IP separada y que un extremo de la línea es el host número 1 y el otro extremo es el host número 2. Siempre que un extremo del enlace serial esté configurado, el SLARP configura automáticamente una dirección IP para el otro extremo.

SMDS
Servicio de datos multimegabit conmutado.

Tecnología WAN de conmutación de paquetes de alta velocidad, ofrecida por una compañía telefónica.

SMTP
Protocolo simple de transferencia de correo (Simple Mail Transfer Protocol).

Estándares de Internet que proporcionan servicios de correo electrónico.

SNMP
Protocolo simple de administración de red.

Estándar que permite supervisar dispositivos individuales en la red. Los dispositivos compatibles con SNMP usan agentes para supervisar una cantidad de parámetros predefinidos para condiciones específicas. Estos agentes recolectan la información y la almacenan en un MIB.

Sobrecarga de NAT
Traduce dinámicamente diversas direcciones locales internas en una única dirección pública, de modo que más de un cliente pueda tener acceso a la conexión con Internet.

Software del sistema operativo de internetworking de Cisco
Ver software IOS de Cisco.

Software IOS de Cisco
Software del sistema operativo de internetworking de Cisco.

Aplicación que proporciona seguridad, escalabilidad y funcionalidad común a todos los productos de Cisco. El software IOS de Cisco permite instalación y administración centralizada, integrada y automatizada de internetworks y, al mismo tiempo, garantiza soporte para una amplia variedad de protocolos, medios, servicios y plataformas.

Software telefónico
Ver telesoftware.

Solicitud de cotización
Ver RFQ.

Solicitud de propuesta
Ver RFP.

Solicitudes de publicación
Información de la VLAN que solicita un cliente VTP si se reinició el switch o si se cambió el nombre de dominio de VTP.

SONET
Red óptica síncrona.

Especificación de red síncrona de alta velocidad (hasta 2.5 Gbps) desarrollada por Bellcore y diseñada para ejecutarse en fibra óptica. El STS-1 es el bloque de creación básico de SONET. Fue aprobado como estándar internacional en 1988.

Soporte de acceso Frame Relay
Ver FRAS.

SP
Proveedor de servicios.

Organización que proporciona servicios de Internet, por ejemplo, la empresa de telefonía local o la compañía de cable.

SPAN
Analizador de puerto conmutado.

Herramienta usada con un switch Catalyst que permite la captura de tráfico al reflejar el tráfico de un segmento conmutado en un puerto SPAN predefinido. Un analizador de red conectado al puerto SPAN puede monitorear el tráfico desde cualquiera de los otros puertos conmutados del switch.

Spanning tree
Subconjunto sin bucles de una topología de red.

SPI
Inspección de paquetes con estado.

Inspecciona y permite que se establezca una respuesta entrante en una red interna.

SPR
Enrutamiento de la ruta libre más corta.

Algoritmo que usa la longitud de la ruta para determinar un spanning-tree hacia la ruta más corta. El enrutamiento hacia la ruta más corta se usa comúnmente en algoritmos de enrutamiento de estado de enlace.

SSH
Secure Shell.

Protocolo dentro de banda usado para encriptar información de nombre de usuario y contraseña cuando se la envía.

SSID
Identificador de conjunto de servicios.

Código de 32 caracteres que normalmente aparece en cada paquete de una transmisión Wi-Fi. El SSID contiene el nombre de red para la WLAN. Todos los dispositivos de una WLAN usan el mismo SSID. El código SSID puede ser configurado por el administrador de la red, o puede ser asignado automáticamente.

SSL
La capa de sockets seguros es un protocolo usado para proteger la información confidencial y los documentos privados en Internet. El SSL usa un sistema criptográfico que utiliza dos claves para encriptar datos: una clave pública o certificado digital, y una clave privada o secreta conocida sólo por el receptor del mensaje.

Stack doble
Dos sistemas con protocolos similares que funcionan simultáneamente en un dispositivo. Por ejemplo, una estrategia de transición de IPv4 a IPv6 consiste en ejecutar ambos stacks de protocolo en el mismo dispositivo. Esto permite que coexistan IPv4 e IPv6.

STDM
Multiplexación estadística por división temporal.

Técnica en la cual la información de múltiples canales lógicos se transmite a través de un solo canal físico. La STDM asigna ancho de banda de forma dinámica sólo a los canales de entrada activos; utiliza mejor el ancho de banda disponible y permite que se puedan conectar muchos dispositivos.

La multiplexación estadística por división temporal también se denomina multiplexación estadística o stat mux.

Storage area network
Ver SAN.

STP
Protocolo Spanning Tree.

Estándares de puente que usan el algoritmo spanning-tree y permiten que un puente evite dinámicamente los bucles que se producen en una topología de red al crear un spanning tree. Un puente intercambia mensajes BPDU con otros puentes para detectar bucles y luego elimina los bucles apagando las interfaces seleccionadas de algunos puentes.

Streaming video
Objetos multimedia que se descargan continuamente en el host receptor mientras un usuario final está viendo el material. El usuario final no descarga por completo el archivo multimedia al equipo.

El streaming media se conoce también como video en vivo.

STS-1
Señal de transporte síncrono de nivel 1.

Formato SONET adoptado por emisoras comunes para circuitos digitales de alta velocidad que operan a 51,84 Mbps.

STS-3c
Señal de transporte síncrono de nivel 3, concatenada.

Formato SONET que especifica la estructura de trama para las líneas de 155,52 Mbps que se usan para transportar celdas de modo de transferencia asíncrona.

STUN
Túnel serial.

Característica del router que permite que dos dispositivos compatibles con SDLC o HDLC se conecten entre sí a través de una topología multiprotocolo arbitraria, usando routers Cisco, en lugar de hacerlo a través de un enlace serial directo.

Subinterfaces
Una de las interfaces virtuales de una sola interfaz física.

Subinterfaz
Una de las interfaces virtuales de una sola interfaz física.

Subred
Sistema de una red IP que comparte una dirección de subred específica. Una subred es segmentada arbitrariamente por el administrador de red para suministrar una estructura de enrutamiento jerárquica, de múltiples niveles, a la vez que resguarda la subred de la complejidad del direccionamiento de las redes conectadas.

Subred no contigua
Dirección de una red separada de las demás por una red o subred.

Sub-subred
Subdivisión de una dirección de una red subdividida.

Sucesor factible
Ruta de respaldo identificada en una tabla de topología. Un sucesor factible se convierte en una ruta de sucesor si falla una ruta principal. El sucesor factible debe tener una distancia declarada menor que la distancia factible de la distancia actual del sucesor hacia el destino.

Sumarización de ruta
Consolidación de direcciones publicadas en una tabla de enrutamiento. La sumarización de ruta reduce la cantidad de rutas de una tabla de enrutamiento, el tráfico de actualización de enrutamiento, y el gasto general de router.

La sumarización de ruta también se conoce como agregación de ruta.

Sumarización manual
Función de una ruta EIGRP mediante la cual el administrador determina qué subredes de qué interfaces se publican como resúmenes de rutas. La sumarización manual se realiza por interfaz y brinda al administrador de red un control completo. En la tabla de enrutamiento, aparece una ruta sumarizada manualmente como una ruta EIGRP obtenida a partir de una interfaz lógica.

Superred
Proceso de resumen de direcciones de clase contiguas establecido por la comunidad de Internet. Un ejemplo de creación de superredes es cuando un grupo direcciones de clase C del 200.100.16.0 al 200.100.31.0 se resume en la dirección 200.100.16.0 con una máscara 255.255.224.0.

También se denomina enrutamiento entre dominios sin clase.

Supervisión remota
Ver RMON.

Suplantación de identidad
1) Método utilizado por un router Cisco para hacer que un host considere una interfaz como si estuviera en ejecución y permitiera una sesión. El router crea respuestas falsas a los mensajes de actividad del host para convencerlo de que la sesión todavía existe. La suplantación de identidad se utiliza en entornos de enrutamiento como DDR. En DDR, se desactiva un enlace conmutado por circuito cuando no hay tráfico para ahorrar gastos de llamada. 2) Cuando un paquete dice provenir de una dirección desde la cual no fue enviado. La suplantación de identidad está diseñada para evitar los mecanismos de seguridad de la red, filtros y listas de acceso.

Sustitución
Técnica de resolución de problemas que utiliza partes en funcionamiento para probar el equipamiento.

SVC
Circuito virtual conmutado.

Ruta que se establece dinámicamente a pedido y es destruida una vez que se completa la transmisión. Los SVC se utilizan cuando la transmisión de datos es esporádica.

Switch
Dispositivo de red que filtra, envía e inunda la red con tramas según la dirección de destino de cada trama. El switch opera en la capa de enlace de datos del modelo de referencia OSI.

Switch de grupo de trabajo Catalyst
Serie de switches de grupo de trabajo de Cisco que mejoran el rendimiento de red de los grupos de trabajo cliente/servidor Ethernet. El switch de grupo de trabajo Catalyst integra las mejoras de software para administración de red y proporciona una interfaz de 100 Mbps a los servidores y estaciones de trabajo de Ethernet a escritorio dedicadas.

Switch de paquetes
Dispositivo WAN que dirige paquetes a lo largo de la ruta más eficiente y permite que múltiples conexiones compartan el canal de comunicaciones.

El switch de paquetes también se conoce como nodo de switch de paquetes.

Switch de red de área local
Ver switch LAN.

Switch LAN
Switch de red de área local.

Dispositivo que envía paquetes entre segmentos de enlace de datos a gran velocidad. Por lo general, un switch de LAN utiliza la dirección MAC para determinar adónde debe enviar el tráfico. Algunos switches de LAN funcionan en el núcleo de la red, mientras que otros funcionan a nivel de grupo de trabajo.

Switch malicioso
Switch no identificado en una red.

Switch multicapa
Dispositivo que filtra y envía paquetes basándose en direcciones MAC y direcciones de red. Un switch de Capa 2/Capa 3 es un switch multicapa.

Switch raíz
Ver puente raíz.

Switches multicapa
Dispositivo que filtra y envía paquetes basándose en direcciones MAC y direcciones de red. Un switch de Capa 2/Capa 3 es un switch multicapa.

Syslog
Tipo de mensaje registrado y enviado a un servidor externo para informar a los usuarios de los distintos informes en tiempo real.

T1
Servicio de portadora de WAN digital que transmite datos con formato DS-1 a 1,544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o sustitución binaria de 8 ceros.

T1 fraccional
Parte de una conexión T1 de gran ancho de banda ofrecida a un cliente por un proveedor de servicios.

T1/E1
Servicio de portadora de WAN digital que transmite datos con formato DS-1 a 1,544 Mbps a través de la red de conmutación telefónica, usando codificación AMI o sustitución binaria de 8 ceros.

T3
Servicio de portadora de WAN digital que transmite datos con formato DS-3 a 44,736 Mbps a través de la red de conmutación telefónica.

Tabla de enrutamiento
Tabla que se almacena en un router o en algún otro dispositivo de internetworking que ayuda a identificar las rutas a los destinos de red y las métricas asociadas con dichas rutas.

Tabla de topología
Una de las tres tablas de un router EIGRP. La tabla de topología enumera todas las rutas aprendidas de cada vecino de EIGRP. DUAL toma la información de las tablas de vecinos y de topología y calcula las rutas de menor costo hacia cada vecino. La tabla de topología identifica hasta cuatro rutas principales sin bucles para cualquier destino.

Tabla de vecinos
Una de las tres tablas de routers EIGRP interconectadas. La tabla de vecinos recopila y enumera información sobre los routers vecinos conectados directamente. Mediante un número de secuencia, se registra el número del último mensaje de saludo recibido de parte de cada vecino y coloca una marca horaria del horario en que llega el paquete. Si no se recibe un paquete de saludo dentro del tiempo de espera, el tiempo vence y DUAL vuelve a calcular la topología. Otras tablas de routers incluyen las tablas de topología y las de enrutamiento.

Tarjeta de interfaz de red de área extensa
Ver WIC.

Tarjeta de interfaz de WAN/de voz
Ver VWIC.

Tarjeta de interfaz WAN
Ver WIC.

Tarjeta de interfaz WAN de alta velocidad
Ver HWIC.

Tc
Tiempo suscrito.

Intervalo de tiempo calculado para que los datos recorran una distancia específica.

TDM
Multiplexación por división temporal.

División del ancho de banda que permite que múltiples señales lógicas se transmitan simultáneamente a través de un solo canal físico. Las señales se separan posteriormente en el extremo receptor.

Teleconferencia
Método para que un grupo de personas pueda comunicarse en línea en tiempo real.

Telefonía
Tecnología diseñada para convertir audio en señales digitales, y para transmitir señales por una red, especialmente redes conmutadas por paquete.

Telefonía de protocolo de Internet
Ver telefonía de IP.

Telefonía IP
Teléfono compatible con llamadas de voz a través de una red IP.

Teléfono de protocolo de Internet
Ver teléfono de IP.

Teléfono IP
Teléfono compatible con llamadas de voz a través de una red IP.

Telesoftware
Aplicación instalada en un equipo que admite llamadas de voz. Un ejemplo de telesoftware es Cisco IP Communicator.

Telnet
Protocolo TCP/IP que permite que un usuario remoto se conecte a un host de la red y emita comandos de forma remota.

Temporización
Velocidad a la que se desplazan los datos en el bucle local.

Temporizador de actualización
Período de tiempo en el que debe utilizarse una entrada antes de que el switch la elimine de la tabla de direcciones MAC.

Temporizador de espera
Colocación de un router en un estado en el que no publica ni acepta rutas por un período específico de tiempo, que se conoce como período de espera. La espera se usa para eliminar la información defectuosa acerca de una ruta de todos los routers de la red. Suele colocarse en espera una ruta cuando falla un enlace de esa ruta.

TFTP
Protocolo de transferencia de archivos trivial.

Estándares que permiten transferir archivos de un equipo hasta otro a través de una red. El TFTP es una versión simplificada del FTP.

Tiempo de actividad
Período en el cual una red o un dispositivo funcionan completamente.

Tiempo de convergencia
Condición donde la velocidad y capacidad de un grupo de dispositivos de internetworking que ejecutan un protocolo de enrutamiento específico reaccionan después de un cambio en la topología. Cuanto más rápido el tiempo de convergencia, más rápidamente puede adaptarse la red a la nueva topología.

Tiempo de espera
Período de tiempo durante el cual un router considera a un vecino destino alcanzable.

Tiempo suscrito
Ver Tc.

Tipo de encapsulación
Transmisión de un protocolo de red dentro de otro. El proceso denominado tunneling es la base de diversos sistemas de seguridad IP, incluido IPsec, utilizado en las VPN.

Tipo de servicio
Ver TOS.

Topología
Mapa de la disposición de nodos y medios de red dentro de una estructura de networking empresarial. La topología puede ser física o lógica.

Topología activa
Diseño de red RSTP que hace que los puertos pasen al estado de reenvío si no están en estado de descarte o si están bloqueados.

Topología en estrella
Estructura en la cual los dispositivos de una red se conectan a un switch central común mediante enlaces punto a punto. La topología en estrella es la topología física usada más comúnmente para LAN Ethernet.

Topología en estrella jerárquica
Sistema de red en el que un switch o router central se conecta a otros switches o routers. El diseño de una topología en estrella jerárquica es similar al hub and spoke de una rueda.

Topología física
Distribución de dispositivos en una red. La topología física muestra la forma en la que los dispositivos están conectados mediante el cableado y la distribución de los cables.

Topología lógica
Mapa del flujo de datos en una red, que muestra cómo los dispositivos se comunican entre sí.

Tormenta de broadcast
Evento de red indeseable en el que se envían muchos broadcasts de manera simultánea a través de todos los segmentos de la red. Una tormenta de broadcast hace uso sustancial del ancho de banda de la red y, por lo general, causa retrasos mayores que los límites de tiempo.

ToS
Tipo de servicio.

Campo de 8 bits usado para clasificación de tramas localizado en el paquete IP y usado por un dispositivo para indicar la precedencia o prioridad de una trama dada. No se utiliza el ToS cuando se recibe una trama que contiene una etiqueta de trama 802.1q.

Trabajador a distancia
Empleado que realiza su trabajo fuera de la oficina centralizada.

Trabajo fuera de la oficina
Trabajo que se realiza fuera de la oficina centralizada.

Traducción de dirección de red dinámica
Ver NAT dinámica.

Traducción de dirección de red estática
Ver NAT estática.

Traducción de la dirección del puerto (PAT)
Ver PAT.

Traducción de la dirección del puerto
Ver PAT.

Traducción de direcciones de red
Ver NAT.

Traducción de direcciones de red: traducción de protocolos
Ver NAT-PT.

Tráfico externo
Comunicación de datos desde una red privada y hasta ella.

Tráfico garantizado
Transferencia de datos a la velocidad especificada para el PVC. La red no debe descartar el tráfico garantizado en condiciones de red normales.

Tráfico interno
Datos transmitidos dentro de una red privada, de confianza.

Tramas unicast
Mensaje que se envía a un solo destino de red.

Transacción atómica
Proceso que garantiza que se lleven a cabo todas las tareas de una transacción en el sistema de una base de datos, o bien que no se lleve a cabo ninguna. La transacción atómica queda anulada si no se lleva a cabo el proceso completo.

Transceptor
Dispositivo que recibe y envía señales analógicas y digitales.

Transferencia de archivos
Aplicación de red utilizada para mover archivos de un dispositivo de red a otro.

Transmisión serial
Método de transmisión de datos en el que los bits de un carácter de datos se transmiten secuencialmente a través de un solo canal.

Transmisión síncrona
Señales digitales que se envían con temporización precisa. Las señales de transmisión síncrona tienen la misma frecuencia, con caracteres individuales en bits de control de inicio y de parada, que designan el comienzo y el fin de cada carácter.

Transparente
No visible o evidente. En networking, un protocolo de capa inferior puede tomar una decisión que no afecte o incluya las capas superiores, por lo tanto la acción es invisible, o transparente para las capas superiores.

Triggered update
Mensaje que contiene la tabla de enrutamiento de un router que se envía a routers vecinos en una red cuando se inicia el router.

TSP
Proveedor de servicios de telecomunicaciones.

Proveedor autorizado por las entidades reguladoras para operar un sistema de telecomunicaciones y proporcionar servicio de telecomunicaciones.

El proveedor de servicios de telecomunicaciones también se denomina operador de intercambio local o portadora.

Túnel
Ruta segura de comunicación entre dos pares, como dos routers.

Túnel serial
Ver STUN.

Tunneling
Método de transmisión de datos por redes con protocolos distintos. Con el tunneling, un paquete de datos es encapsulado para formar un nuevo paquete que cumple con los protocolos que se utilizan en las redes intermediarias.

Tunneling dividido
Configuración para otorgar a un cliente VPN acceso a Internet mientras se establece un túnel por un Router Cisco IOS. Se necesita tunneling dividido para otorgar a un cliente VPN acceso seguro a recursos corporativos a través de IPSec, además de proporcionarle acceso no seguro a Internet.

TxQ
Cola de transmisión.

Proceso de almacenamiento de tráfico en hardware para luego enviar los paquetes en el orden en el que fueron recibidos.

UDP
Protocolo de datagramas del usuario.

Estándar para la transmisión sin conexión de tráfico de voz y video. Las transmisiones con UDP no se ven afectadas por los retrasos causados por los acuses de recibo y la retransmisión de paquetes perdidos.

Umbral
Nivel aceptable de errores en una interfaz.

Unicast
Mensaje que se envía a un solo destino de red.

Unidad de bastidor
Ver RU.

Unidad de control multipunto
Ver MCU.

Unidad de datos del protocolo de puentes
Ver BPDU.

Unidad de servicio de canal
Ver CSU.

Unidad de servicio de canal/unidad de servicio de datos
Ver CSU/DSU.

Unidad de servicio de datos
Ver DSU.

Unidad máxima de transmisión
Ver MTU.

Unión Internacional de Telecomunicaciones
Ver ITU-T.

UplinkFast
Mejora del STP que minimiza el tiempo de inactividad ocasionado por los cálculos. El UplinkFast de STP acelera la elección de un nuevo puerto raíz cuando hay fallas en un enlace o switch, o cuando se reconfigura un STP. La transición del puerto raíz al estado de reenvío ocurre inmediatamente, sin pasar por los procedimientos normales de STP de escucha y aprendizaje.

UPS
Fuente de energía ininterrumpible.

Fuente de energía continua y fiable puesta a disposición en caso de un corte de energía. Generalmente, se proporcionan UPS para servidores y dispositivos de red críticos.

V.35
Estándar de la UIT-T que describe un protocolo de la capa física, síncrono, que se utiliza para las comunicaciones entre un dispositivo de acceso de red y una red de paquetes. V.35 es el estándar de uso más generalizado en Estados Unidos y en Europa, y se recomienda para velocidades de hasta 48 kbps.

Valor de umbral
Cantidad máxima de errores que un switch permite antes de pasar a la conmutación de almacenamiento y reenvío para disminuir el tráfico y corregir el problema.

Valor K
Valor numérico para que una fórmula métrica compuesta en EIGRP determine el mejor camino a un destino. K1 y K3 se establecen en 1. K2, K4 y K5 se establecen en 0. El valor de 1 indica que el ancho de banda y el retraso tienen igual peso.

Variación
Número multiplicado por una ruta para determinar si está dentro de la métrica aceptable máxima para usarlo como ruta. Por ejemplo, si el valor de la variación es 2, el router balancea la carga de tráfico usando cualquier ruta para la cual la métrica sea menos de dos veces la mejor métrica.

VC
Circuito virtual.

Relación lógica que se crea para garantizar la comunicación confiable entre dos dispositivos de red. Un circuito virtual se define por un par identificador de ruta virtual/identificador de canal virtual, y puede ser tanto un circuito virtual permanente como un circuito virtual conmutado. Los circuitos virtuales se usan en Frame Relay y X.25. En ATM, un circuito virtual se denomina canal virtual.

Vecino
En OSPF, routers que tienen interfaces en una red común. En una red de acceso múltiple, los vecinos se detectan de forma dinámica a través del protocolo de saludo OSPF.

Vector
Segmento de datos de un mensaje SNA. El vector está compuesto por un campo de longitud, una clave que describe el tipo de vector y datos específicos del vector.

Vector distancia
Tipo de protocolo de enrutamiento que informa de manera periódica a los routers con conexión directa los cambios que se producen en la red.

Velocidad de acceso local
La velocidad medida por reloj, o velocidad de puerto, de la conexión del bucle local a la nube Frame Relay.

Velocidad de cable
Velocidad con la que se envían paquetes en una red.

Velocidad de información suscrita
Ver CIR.

Velocidad excesiva
Tráfico de una red que supera la velocidad garantizada de una conexión determinada. El tráfico excesivo se envía sólo si los recursos de la red están disponibles. El tráfico excesivo puede descartarse durante los períodos de congestión. La velocidad excesiva es igual a la velocidad máxima menos la velocidad garantizada.

VID
ID de la VLAN.

Identidad de la VLAN insertada en una trama Ethernet al entrar a un puerto de un switch.

Video a pedido (Video On Demand)
Ver VoD.

VLAN
Red de área local virtual.

Grupo de dispositivos alojados en una red, generalmente estaciones de usuarios finales, que se comunican como si estuvieran conectados al mismo segmento de la red aún cuando pueden estar en segmentos distintos. Las VLAN se configuran en switches de grupo de trabajo. Los switches con VLAN pueden interconectarse usando protocolos VLAN de enlace troncal.

La VLAN también se denomina LAN virtual.

VLAN de administración
Red de área virtual local de administración.

VLAN1 de un switch. La dirección IP de VLAN1 se utiliza para tener acceso remoto al switch y configurarlo, y para intercambiar información con otros dispositivos de red.

VLAN nativa
VLAN especial que aloja el tráfico sin etiquetar. Los enlaces troncales transmiten el tráfico sin etiquetas a través de la VLAN nativa. En switches Catalyst de Cisco, VLAN1 es la VLAN nativa.

VLSM
Máscara de subred de longitud variable.

Técnica utilizada para especificar una máscara de subred distinta para el mismo número de red principal, a fin de identificar distintas subredes. Las VLSM pueden ayudar a optimizar el espacio de dirección IP disponible.

VMPS
Servidor de política de administración de VLAN.

Servidor que contiene una base de datos que asigna direcciones MAC a la VLAN. Cuando se conecta un dispositivo a un puerto del switch, el VMPS busca en la base de datos una coincidencia con la dirección MAC, y asigna ese puerto de forma temporal a la VLAN correspondiente.

VoD
Video a pedido.

Tipo de sistema que permite que un usuario seleccione y vea contenido de video a través de una red como parte de un sistema de televisión interactivo. Un sistema de VoD proporciona el contenido mediante streams, y permite la reproducción mientras se descarga el video, o bien descarga el contenido por completo a la caja del equipo antes de comenzar a reproducirlo.

VoIP
Protocolo de voz por Internet.

Estándar para transmitir datos de voz encapsulados en un paquete IP de una red IP ya implementada sin necesidad de tener su propia infraestructura de red. En VoIP, el procesador de señales digital divide la señal de voz en tramas que se agrupan por pares y son almacenadas en paquetes de voz. Los paquetes de voz se transportan mediante IP según la especificación H.323 de ITU-T.

El VoIP también se denomina voz sobre IP.

Voz sobre IP
Ver VoIP.

VPC
Conexión de ruta virtual.

Grupo de conexiones de canal virtual que comparten una o más VPL contiguas.

VPL
Enlace de ruta virtual.

Grupo de enlaces de canales virtuales unidireccionales dentro de una ruta virtual con los mismos puntos finales. Al agruparlos en VPL, se reduce la cantidad de conexiones que se deben administrar, con lo cual se reducen el costo y el tráfico de control de la red.

VPN
Red privada virtual.

Red por la cual se envían datos a través de una infraestructura de telecomunicaciones pública y se mantiene la privacidad de los datos mediante la creación de un túnel en la infraestructura de telecomunicaciones pública.

VPN de acceso remoto
Opción de conectividad utilizada para aumentar o reemplazar la estrategia tradicional de acceso remoto, tal como el uso de un enlace dial-up.

La VPN de acceso remoto también se denomina VPN de usuario remoto.

VPN de sitio a sitio
Conexión entre sitios de una organización o entre una organización y un sitio asociado. La VPN sitio a sitio no requiere configuración de cliente IPSec en los equipos hosts porque los datos se encriptan en el punto de entrada de un sitio y se desencriptan en el punto de salida del túnel del otro sitio.

VTP
Protocolo de enlace troncal virtual

Estándar propiedad de Cisco que mantiene una configuración unificada de VLAN dentro de un dominio administrativo común.

VWIC
Tarjeta de interfaz de WAN/de voz.

Adaptador que admite aplicaciones de voz, datos y voz integrados, y datos. La VWIC facilita la migración de datos, así como de datos y voz canalizados, a soluciones de paquetes de voz, lo cual simplifica la distribución y la administración.

WAN
Red de área extensa.

Red de comunicación de datos que sirve a usuarios dentro de un área geográficamente extensa y a menudo usa dispositivos de transmisión provistos por un servicio público de comunicaciones. Entre los ejemplos de tecnología WAN se cuentan Frame Relay, SMDS y X.25.

WEP
Privacidad equivalente por cable.

Estándar de mecanismo de seguridad opcional definido dentro del estándar 802.11, diseñado para equiparar la integridad de enlace de los dispositivos inalámbricos con la del cable.

WIC
Tarjeta de interfaz de red de área extensa.

Adaptador que conecta un sistema a un proveedor de servicios de enlace de WAN.

WLAN
Red de área local inalámbrica.

Conexión entre dos o más equipos sin utilizar medios físicos. La WLAN usa la comunicación por radio para lograr la misma funcionalidad que la LAN

La WLAN también se denomina LAN inalámbrica.

WPA
Acceso protegido Wi-Fi.

Estándar basado en IEEE 802.11i que fue desarrollado para abordar los problemas relativos a la seguridad. La WPA proporciona un mayor nivel de seguridad en una red inalámbrica. Utiliza el protocolo de integridad de clave temporal para la protección de datos y 802.1X para la administración de claves autenticadas.

Zona de autoridad
Sección del árbol de nombre de dominio bajo la autoridad de un servidor de nombres. La zona de autoridad está asociada con el DNS.

Zona desmilitarizada
Ver DMZ.

CISCO

Guía Portátil Cisco

CCNA Discovery

Diseño y soporte de redes de computadoras

Versión 4.0

Su *Guía Portátil Cisco* de Cisco Networking Academy es una forma de leer el texto del curso sin estar conectado a Internet.

Gracias a su diseño como recurso de estudio, puede leer, resaltar y repasar con facilidad mientras se desplaza de un lado a otro, en donde no haya una conexión disponible a Internet:

- El texto se extrae de manera directa, palabra por palabra, del curso en línea, para que usted pueda resaltar los puntos importantes.
- Los encabezados con su correlación exacta de página ofrecen una rápida referencia al curso en línea para su análisis en el salón de clases y al prepararse para los exámenes.
- Un sistema de iconos lo lleva al plan de estudios en línea, para que aproveche al máximo las imágenes, laboratorios, actividades de Packet Tracer y las actividades dinámicas basadas en Flash que están incrustadas dentro de la interfaz del curso en línea de la Cisco Networking Academy.

Refiera a la Figura del curso en línea | Refiera a la actividad de laboratorio del curso en línea | Refiera a la actividad de "Packet Tracer" del curso en línea | Refiera al Gráfico Interactivo del curso en línea | Vaya al curso en línea y complete la prueba

La *Guía Portátil Cisco* es un recurso rápido, con un enfoque en el ahorro de papel, que lo ayudará a alcanzar el éxito en el curso en línea de Cisco Networking Academy.

ISBN 978-607-32-0426-2
90000
9 786073 204262

Cisco | Networking Academy®
Mind Wide Open™

ciscopress.com